ADSL 2/2+ VoIP Router

IAD-300

User's Manual

Copyright

Copyright© 2008 by PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution

To assure continued compliance (example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions: (1) This device may not cause harmful interference, and (2) this Device must accept any interference received, including interference that may cause undesired operation.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)
The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

WEEE Regulation

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

Revision

User's Manual for ADSL 2/2+ VoIP Router
Model: IAD-300
Rev: 1.0 (Nov. 2008)
Part No. EM-IAD300_v1

Table of Contents

1. INTRODUCTION **8**

1.1 Feature ***8***

1.2 Package Contents ***10***

1.3 Physical Details ***10***

2. INSTALLATION **12**

2.1 System Requirement ***12***

2.2 Hardware Installation ***12***

2.3 Configuring the Network Properties ***13***

3. WEB CONFIGURATION MANAGEMENT **17**

3.1 Quick Setup ***18***

3.1.1 WAN Interface Setup 18

3.1.1.1 Setup VPI/VCI and QoS 18

3.1.1.2 Select Internet Connection Type and Encapsulation Type 19

3.1.1.3 Internet Connection Type-PPP over ATM (PPPoA) 20

3.1.1.4 Internet Connection Type-PPP over Ethernet (PPPoE) 21

3.1.1.5 Internet Connection Type-MAC Encapsulation Routing (MER) 23

3.1.1.6 Internet Connection Type-IP over ATM (IPoA) 25

3.1.1.7 Internet Connection Type-Bridging 27

3.1.2 LAN Interface Setup 28

3.1.3 WAN Setup Summary 29

3.1.4 Quick Setup Completed 30

3.2 DSL Router Device information ***31***

3.2.1 Summary of Device information 31

3.2.2 WAN Interface information 32

3.2.3 Statistics 33

3.2.3.1 Statistics of LAN 33

3.2.3.2 Statistics of WAN 34

3.2.3.3 Statistics of ATM 35

3.2.3.4 Statistics of ADSL 37

3.2.4 Route table information 39

3.2.5 ARP table information 40

3.2.6 DHCP IP Leases information 40

3.3 Advanced Setup ***41***

3.3.1 WAN CONFIGRATION 41
3.3.1.1 Add PPPoE PVC 43
3.3.1.2 Add PPPoA PVC 48
3.3.1.3 Add MER PVC 53
3.3.1.4 Add IPoA PVC 58
3.3.1.5 Add Bridge PVC 63
3.3.2 LAN configuration 66
3.3.3 NAT-- Network Address Translation 69
3.3.3.1 NAT -- Virtual Servers Setup 71
3.3.3.2 Port Triggering 74
3.3.3.3 DMZ Host 76
3.3.4 Security 78
3.3.4.1 Outgoing IP Filtering Setup 79
3.3.4.2 Incoming IP Filtering Setup 82
3.3.4.3 MAC Filtering Setup 85
3.3.5 Quality of Service 87
3.3.5.1 Enable QOS 87
3.3.5.2 QOS--Queue Config 88
3.3.5.3 QoS -- QoS Classification 90
3.3.6 Routing 95
3.3.6.1 Routing – Default Gateway 95
3.3.6.2 Static Routes 96
3.3.6.3 RIP 97
3.3.7 DNS 99
3.3.7.1 DNS Server 99
3.3.7.2 Dynamic DOMAIN NAME SERVICE (DDNS) 100
3.3.8 DSL 102
3.3.9 Print Server 103
3.3.9.1 Configuring Print Server on DSL Server 103
3.3.9.2 Configuring Print Server on the Windows Host 104
3.3.10 Port Mapping 107
3.3.10.1 Create a new mapping group 108
3.3.10.2 Edit a existing group 109
3.3.11 Certificate 110

3.3.11.1 Create New Local Certificate 110
3.3.11.2 Import Existing Local Certificate 112
3.3.11.3 Trusted CA Certificates 113
3.4 Voice ***114***
3.4.1 SIP Basic Setting 115
3.4.2 SIP Advanced Setting 119
3.4.3 VoIP functionality 122
Registering. 122
Placing a call 122
Anonymous call 122
Do not disturb (DND) 123
Redial. 123
Call return. 123
Call hold 123
Call waiting. 123
Blind transfer 123
Consultative transfer 124
Call forwarding no answer 124
Call forwarding busy 124
Call forwarding all 124
3-Way conference 125
T38 Faxing 125
Pass-through Faxing 125
PSTN to VoIP call 125
3.5 USB Storage ***126***
3.5.1 FTP Server Configure 126
3.5.2 FTP Client Setting 127
3.6 Diagnostics ***128***
3.7 Management ***129***
3.7.1 Settings 129
3.7.1.1 Settings Backup 129
3.7.1.2 Settings Update 129
3.7.1.3 Settings Restore Default 129
3.7.2 System Log 130

3.7.3 SNMP Client 133
Configure 135
3.7.4 TR-69 Client Management 136
3.7.5 Internet Time 137
3.7.6 Access Control 138
3.7.6.1 Access Control – Services 138
3.7.6.2 Access Control -- IP Addresses 138
3.7.6.3 Access Control – Passwords 139
3.7.7 Update Software 140
3.7.8 Save/Reboot 140
APPENDIX A: GLOSSARY 141

1. Introduction

The PLANET ADSL 2/2+ VoIP Router - IAD-300, provide ISP or residential Home Users the ideal solution for sharing a high-speed ADSL 2/2+ broadband Internet connection on 4-Port 10/100Base-TX Fast Ethernet backbone and also with the capability to make the VoIP calls through Internet. The IAD-300 can support downstream transmission rates of up to 24Mbps and upstream transmission rates of up to 3.5Mbps. It supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), PPP over Ethernet (RFC 2516), RFC 1483 encapsulation over ATM (MER, bridged or routed), and IPoA (RFC1577) to establish a connection with ISP.

Via the User-Friendly management interface, IAD-300 can be managed by workstations running standard web browsers. Furthermore, IAD-300 provides DHCP Server, Virtual Server, DMZ, Access Control, IP Filter, VPN Pass-Through, DDNS, Printer Server and UPnP capability.

The IAD-300 also serves as an Internet firewall, protecting your network from being accessed by outside users. Besides, the IAD-300 provides high quality Voice over Internet Protocol (VoIP), the SIP (RFC3261) protocol offers the capability to make the call in a cost-effective way, either through Internet or local phone system.

1.1 Feature

Internet Access Features

- ***Shared Internet Access*** All users on the LAN can access the Internet through the IAD-300 using only a single external IP Address. The local (private) IP Addresses are hidden from external sources. This process is called NAT (Network Address Translation).
- ***Built-in ADSL 2/2+ Modem*** The IAD-300 provides ADSL 2/2+ modem, and supports all common ADSL connections.
- ***PPPoE, PPPoA, Direct Connection Support*** Various WAN connections are supported by IAD-300.
- ***Auto-detection of Internet Connection Method*** In most situations, the IAD-300 can test your ADSL and Internet connection to determine the connection method used by your ISP.
- ***Fixed or Dynamic IP Address*** On the Internet (WAN port) connection, the IAD-300 supports both Dynamic IP Address (IP Address is allocated on connection) and Fixed IP Address.

VoIP Functions

- ***SIP 2.0 Support*** IAD-300 supports SIP2.0 for the compatibility of most popular VoIP telephone server provider and SIP proxy gateway.
- ***Most SIP Proxy Server support*** IAD-300 compatible with known popular Internet SIP Proxy provider like FWD and Infonex.
- ***Lifeline Support*** In case of unexpected Internet error or power failure, you still can make the regular PSTN call with Lifeline support.
- ***Two FXS Interface*** IAD-300 supports two FSX interface that can connect to any traditional analog telephone for Internet Call through the Internet Telephony Service Provider. It also makes the local PSTN phone call directly.

Advanced Internet Functions

- ***Virtual Servers*** This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.
- ***DMZ Support*** IAD-300 can translate public IP addresses to private IP address to allow unrestricted 2-way communication with Servers or individual users on the Internet. This provides the most flexibility to run programs, which could be incompatible in NAT environment.
- ***Firewall*** Supports simple firewall with NAT technology and provides option for blocking access from Internet, like Web, FTP, Telnet, SNMP, and ICMP. It also supports MAC and IP filtering.
- ***Universal Plug and Play (UPnP)*** UPnP allows automatic discovery and configuration of the Broadband Router. UPnP is supported by Windows ME, XP, or later.
- ***VPN Pass through Support*** PCs with VPN (Virtual Private Networking) software are transparently supported - no configuration is required.
- ***RIP1/2 Routing*** It supports RIPv1/2 routing protocol for routing capability.
- ***Simple Network Management Protocol (SNMP)*** It is an easy way to remotely manage the router via SNMP.
- ***Dynamic DNS Support*** DDNS, when used with the Virtual Servers feature, allows users to connect to Servers on your LAN using a Domain Name, even if you have a dynamic IP address which changes every time you connect.
- ***FAX Support*** IAD-300 supports T.38 and G.711 Fax standards.
- ***QoS*** IAD-300 builds Quality of Service in the device for excellent voice quality.

LAN Features

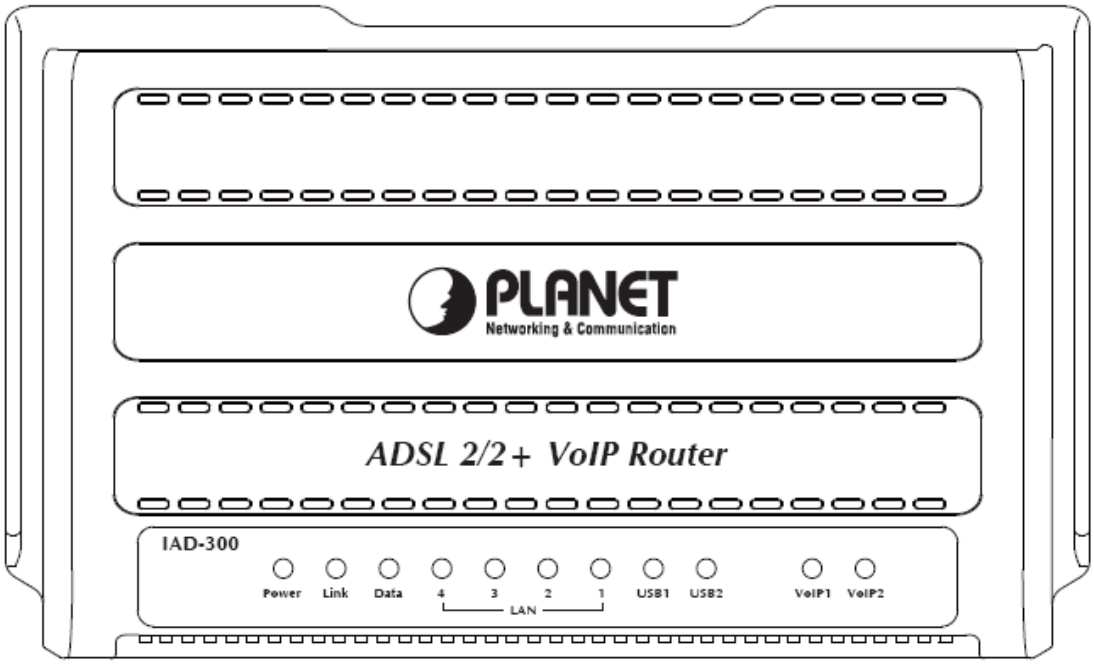
- ***4-Port Switch*** The IAD-300 incorporates a 4-Port 10/100Base-TX switching hub, making it easy to create or extend your LAN.
- ***DHCP Server Support*** **D**ynamic **H**ost **C**onfiguration **P**rotocol provides a dynamic IP address to PCs and other devices upon request. The IAD-300 can act as a DHCP Server for devices on your local LAN.

1.2 Package Contents

- IAD-300 Unit x 1
- Power Adapter x 1
- Quick Installation Guide x 1
- User's Manual CD x 1
- RJ-11 cable x 2
- RJ-45 cable x 1
- Splitter x 1
- USB Cable x 1

1.3 Physical Details

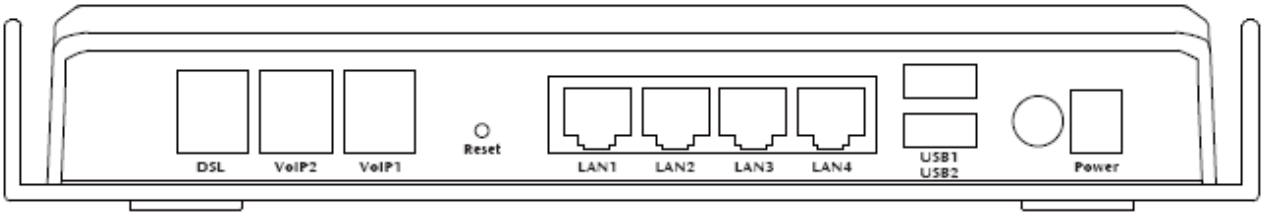
Front Panel of IAD-300



Front Panel LED definition

LED	State	Description
Power	ON	When the router is powered on and in ready state
	OFF	When the router is powered off
Link	ON	Successful connection between ADSL modem and telecom's network
	Flashing	Modem is trying to establish a connection to telecom's network
Data	Flashing	Data is transferred between Router and Internet.
LAN 1-4	ON	Link
	Flashing	TX or RX activity
USB1	ON	The USB Storage device connects to USB1
USB2	ON	The USB Printer connects to USB2
VoIP1/2	ON	VoIP Phone is registered
	Flashing	Phone call is off-hook
	OFF	VoIP Phone is not registered

Rear Panel



Rear Panel Port and Button Definition

Connector	Description
POWER Button	The Power Button is for turn on or turn off the router.
Power	Power connector with 12V DC 2A
USB1	Connect to USB Storage device to USB1 for FTP application.
USB2	Connect your Printer to USB2, the IAD-300 supports the built-in Printer Server.
LAN 1-4	Router is successfully connected to a device through the corresponding port (1, 2, 3, or 4). If the LED is flashing, the Router is actively sending or receiving data over that port.
Reset	The reset button can restore the default settings of device. To restore factory defaults, keep the device powered on and push a paper clip into the hole. Press down the button over 5 seconds and then release.
VoIP 1/2	Connect to any analog telephone for VoIP application.
DSL Line	The RJ-11 connector allows data communication between the modem and the ADSL network through a twisted-pair phone wire.

2. Installation

This chapter offers information about installing your router. If you are not familiar with the hardware or software parameters presented here, please consult your service provider for the values needed.

2.1 System Requirement

1. Personal computer (PC)
2. Pentium III 266 MHz processor or higher
3. 128 MB RAM minimum
4. 20 MB of free disk space minimum
5. RJ45 Ethernet Port

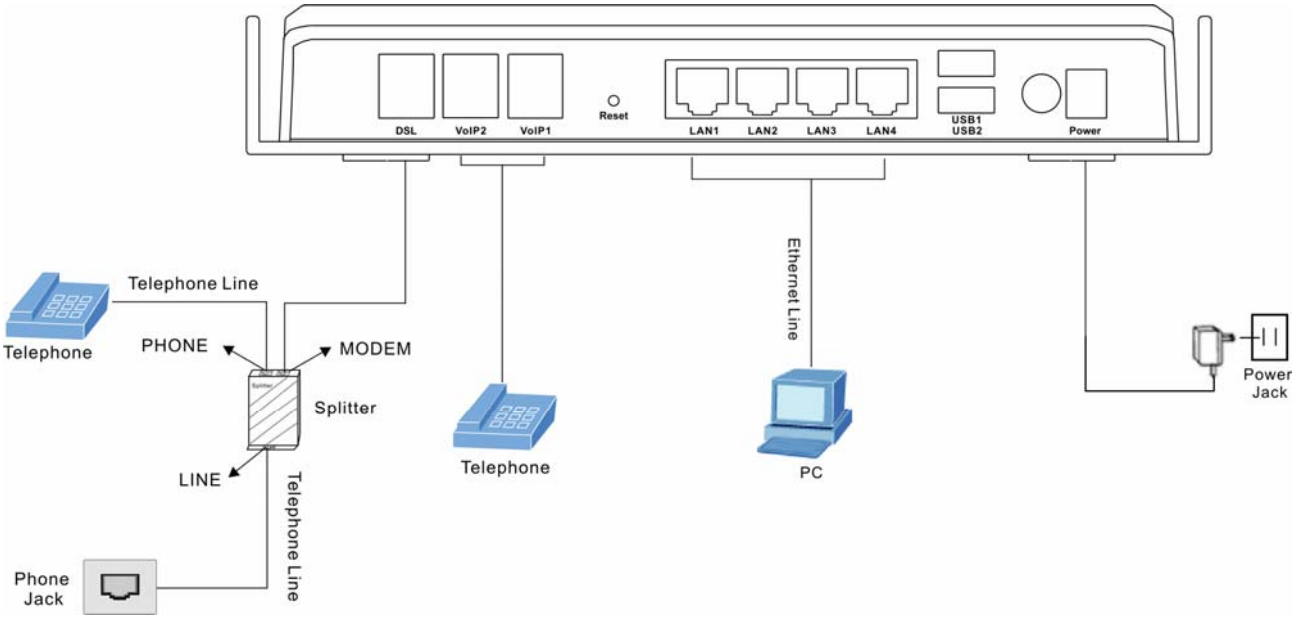
2.2 Hardware Installation

The DSL Router maintains three separate interfaces, the Ethernet LAN, the VoIP FXS Port and an ADSL (WAN) interface. Place the Router in a location where it can be connected to the various devices as well as to a power source. The Router should not be located where it will be exposed to moisture or excessive heat. Make sure the cables and power cord are placed safely out of the way so they do not create a tripping hazard. As with any electrical appliance, observe common sense safety procedures.

The Router can be placed on a shelf or desktop, ideally you should be able to see the LED indicators on the front if you need to view them for troubleshooting.

Please connect the device to you computer as follow:

- If connecting to the splitter, connect the “Line” splitter to wall jack using one telephone cable
- Use another telephone cable to connect “MODEM” port of the splitter and “LINE” port of the modem. The “Phone” port of the splitter can be use to connect the telephone by a telephone cable.
- Use Ethernet cable to connect “LAN” port of the Router and network adaptor of your computer.



If do not need to connect to the splitter,

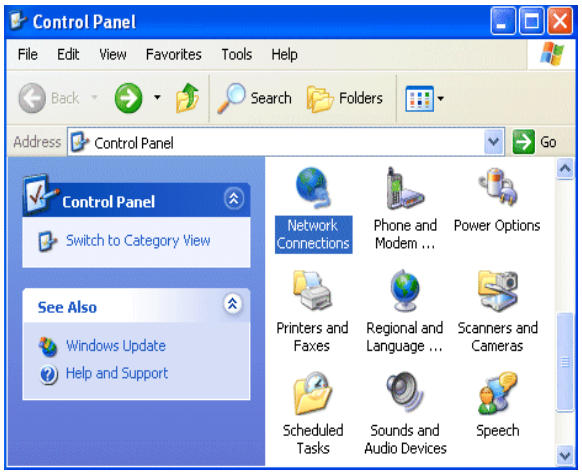
- Connect the modem to wall jack with a telephone cable directly.
- Use Ethernet cable to connect “LAN” port of the modem and network adaptor of your computer.

2.3 Configuring the Network Properties

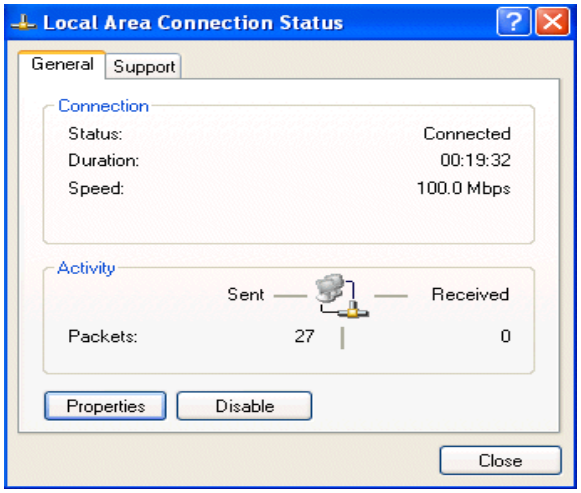
Configuring PC in Windows XP

1. Go to **Start / Control Panel (in Classic View)**. In the Control Panel, double-click on **Network Connections**

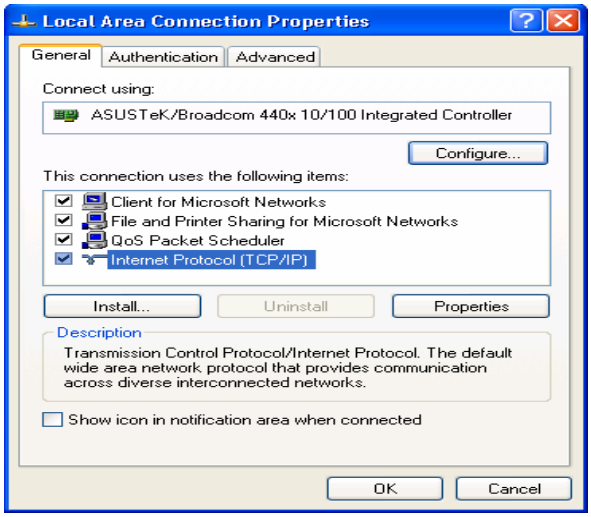
2. Double-click **Local Area Connection**.



3. In the **Local Area Connection Status** window, click **Properties**.

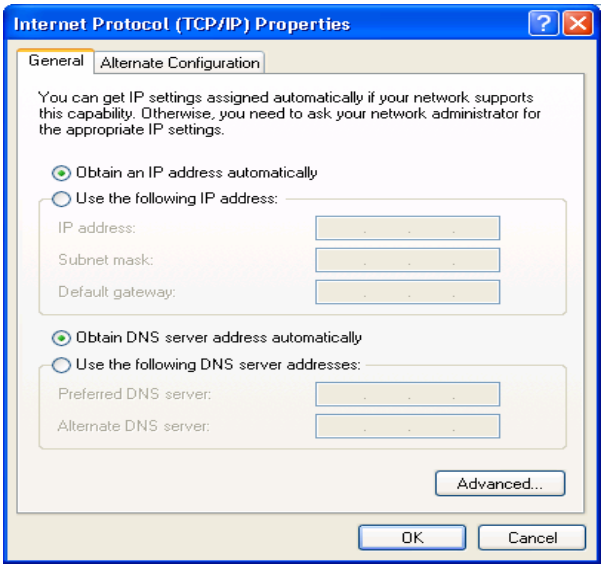


4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



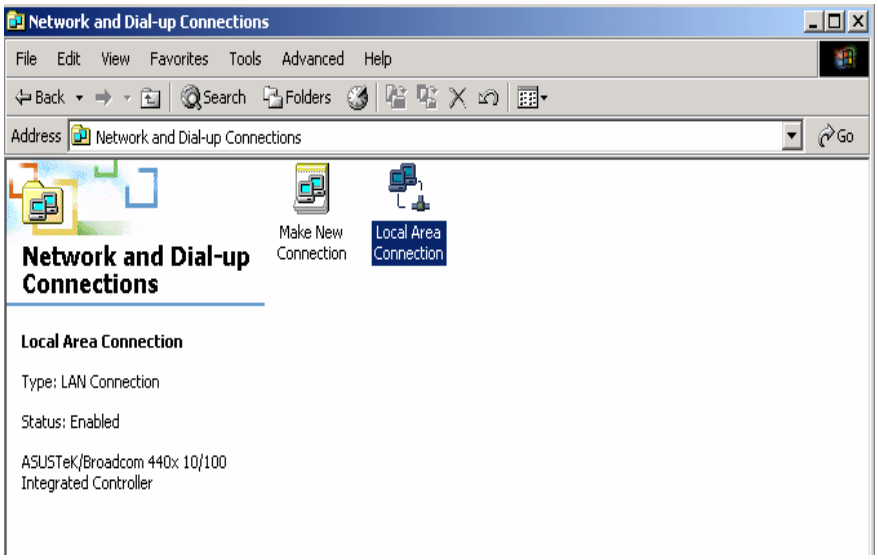
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.

6. Click **OK** to finish the configuration.

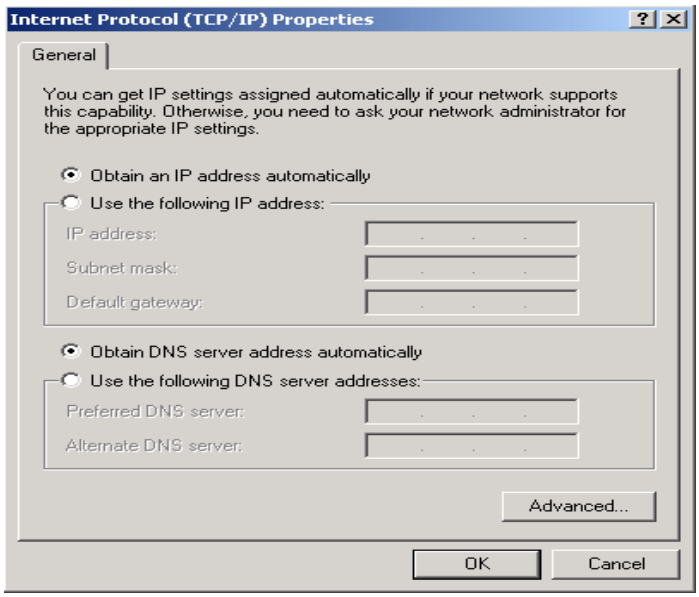

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Configuring PC in Windows 2000

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network and Dial-up Connections**.
2. Double-click **Local Area Connection**.

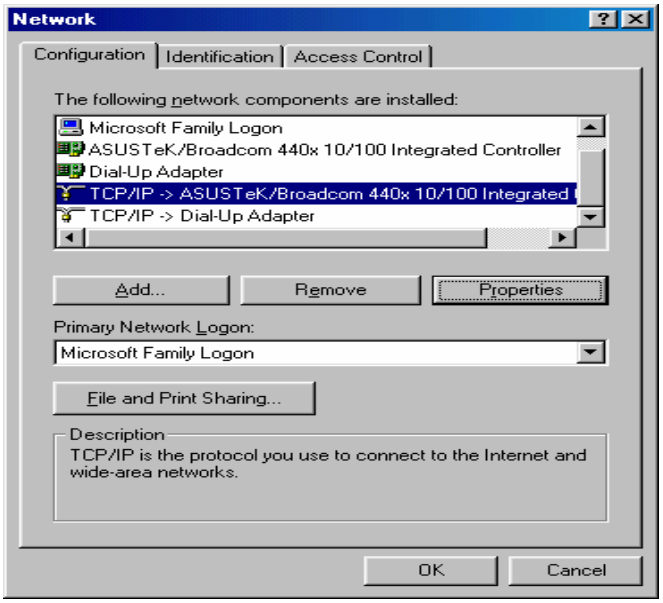


3. In the **Local Area Connection Status** window click **Properties**.
4. Select **Internet Protocol (TCP/IP)** and click **Properties**.
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
6. Click **OK** to finish the configuration.

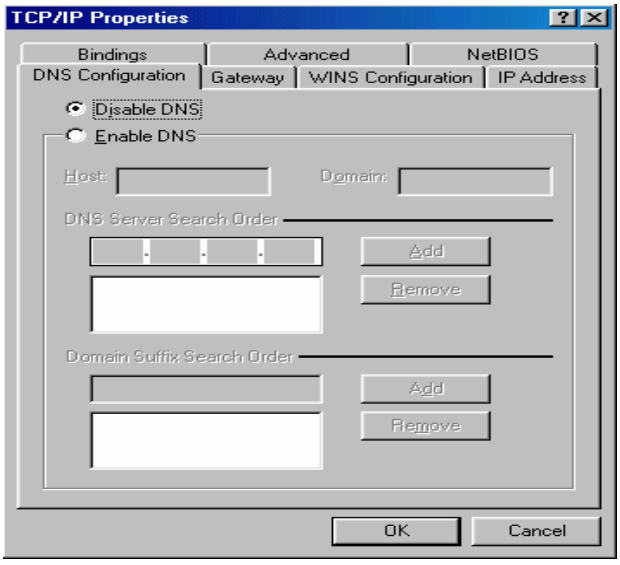

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Configuring PC in Windows 98/Me

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Configuration** tab.
2. Select **TCP/IP** → the name of your Network Interface Card (NIC) in your PC.



3. Select the **Obtain an IP address automatically** radio button.
4. Then select the **DNS Configuration** tab.
5. Select the **Disable DNS** radio button and click **OK** to finish the configuration.



3. Web Configuration Management

Determine your connection settings

Before you configure the router, you need to know the connection information supplied by your ADSL service provider.

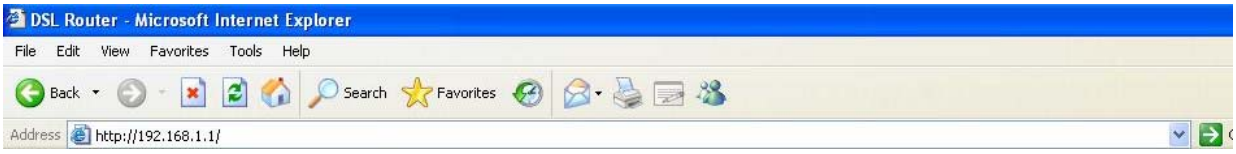
Connecting the ADSL Router to your network

Unlike a simple hub or switch, the setup of the ADSL Router consists of more than simply plugging everything together. Because the Router acts as a DHCP server, you will have to set some values within the Router, and also configure your networked PCs to accept the IP Addresses the Router chooses to assign them.
Generally there are several different operating modes for your applications. And you can know which mode is necessary for your system from ISP. These modes are router, bridge, PPPoE+NAT, and PPPoA+NAT.

Configuring with Web Browser

It is advisable to change the administrator password to safeguard the security of your network.

To configure the router, open your browser, type **"http: //192.168.1.1"** into the address bar and click **"Go"** to get to the login page.
Save this address in your Favorites for future reference.



In login dialog, enter **"admin"** as user name and **"admin"** as default password. After log in, you will see the following page. The default screen is **Quick Setup** setting screen. You can configure the device step by step.

3.1 Quick Setup

When we enter into Quick Setup page, it mainly includes two functions to do.

- **WAN Interface setup**
- **LAN Interface setup**

'Quick Setup' enables speedy and accurate configuration of your Internet connection and other important parameters. The following sections describe these various configuration parameters. Whether you configure these parameters or use the default ones, click **'Next'** to enable your Internet connection.

When subscribing to a broadband service, you should be aware of the method by which you are connected to the Internet. Your physical WAN device can be either Ethernet, DSL, or both. Technical information regarding the properties of your Internet connection should be provided by your Internet Service Provider (ISP). For example, your ISP should inform you whether you are connected to the Internet using a static or dynamic IP address, or what protocols, such as PPPOA or PPPoE, you will be using to communicate over the Internet.

3.1.1 WAN Interface Setup

In WAN Interface Setup phase, we mainly setup PVC and the property of this PVC:

- VPI
- VCI
- Qos
- Internet Connection Type
- Encapsulation Type
- IGMP service
- NAT

3.1.1.1 Setup VPI/VCI and QoS

After logging into the DSL router, When we were not config any PVC at privious time and we have not default settings include PVC,you will see a “**Quick Setup**” web page, which will include some basic configuration that is needed by ATM PVC. the following introductions will guide you through the steps necessary to configure your DSL Router.

According to your Internet service providers (ISP) instructions, specify the following parameters:

■VPI (Virtual Path Identifier):
The virtual path between two points in an ATM network and its valid value is from 0 to 255.

■VCI (Virtual Channel Identifier):
The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols).

■Enable Quality Of Service:
Enabling QoS for PVC improves performance for selected classes of applications. However, since QoS also consumes system resources, the number of PVCs will be reduced consequently. Use Advanced Setup/Quality of Service to assign priorities for the applications.

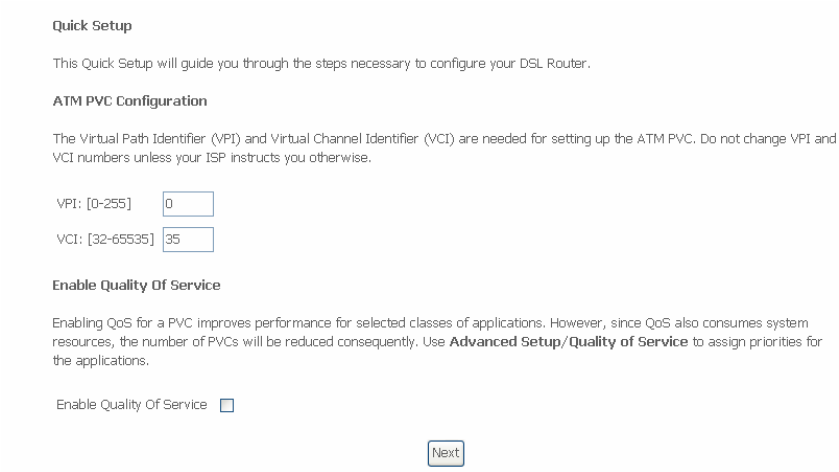

Quick Setup
This Quick Setup will guide you through the steps necessary to configure your DSL Router.
ATM PVC Configuration
The Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) are needed for setting up the ATM PVC. Do not change VPI and VCI numbers unless your ISP instructs you otherwise.
VPI: [0-255] 0
VCI: [32-65535] 35
Enable Quality Of Service
Enabling QoS for a PVC improves performance for selected classes of applications. However, since QoS also consumes system resources, the number of PVCs will be reduced consequently. Use Advanced Setup/Quality of Service to assign priorities for the applications.
Enable Quality Of Service
Next

Figure: PVC and Qos config page

For example, PVC 0/35 is required to modify, so QoS will remain default values. In actual applications, you can modify them depending on your ISP told you.

3.1.1.2 Select Internet Connection Type and Encapsulation Type

You can select your connection type from the following list; each connection type has its Encapsulation Type:

- **PPP over ATM (PPPoA)**
  PPPoA Encapsulation Mode: VC/MUX and LLC/ENCAPSULATION
- **PPP over Ethernet (PPPoE)**
  PPPoE Encapsulation Mode: LLC/SNAP-BRIDGING and VC/MUX
- **MAC Encapsulation Routing (MER)**
  MER Encapsulation Mode: LLC/SNAP-BRIDGING and VC/MUX
- **IP over ATM (IPoA)**
  IPoA Encapsulation Mode: LLC/SNAP-ROUTING and VC/MUX
- **Bridging**
  Bridging Encapsulation Mode: LLC/SNAP-BRIDGING and VC/MUX

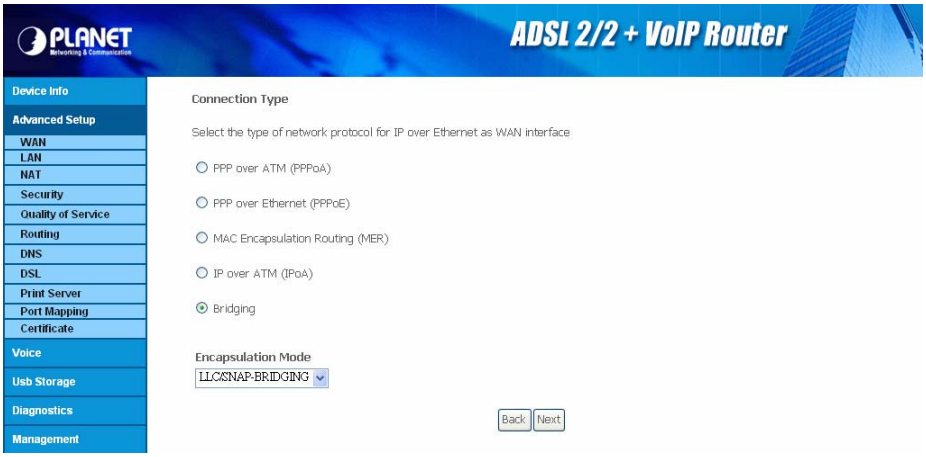


Figure: Internet Connection Type and Encapsulation Type page

For example, Change the connection type of PVC 0/35 to "**bridge**". Select "**bridging**", and "**LLC/SNAP-BRIDGING**" (depending on the uplink equipment, generally "LLC/SNAP-BRIDGING") as "**Encapsulation Mode**".

3.1.1.3 Internet Connection Type-PPP over ATM (PPPoA)

A. Setup the PVC and Qos

B. Select 'PPP over ATM (PPPoA)' from the 'Connection Type' box and It's Encapsulation Type from the ' Encapsulation Mode' combo box:

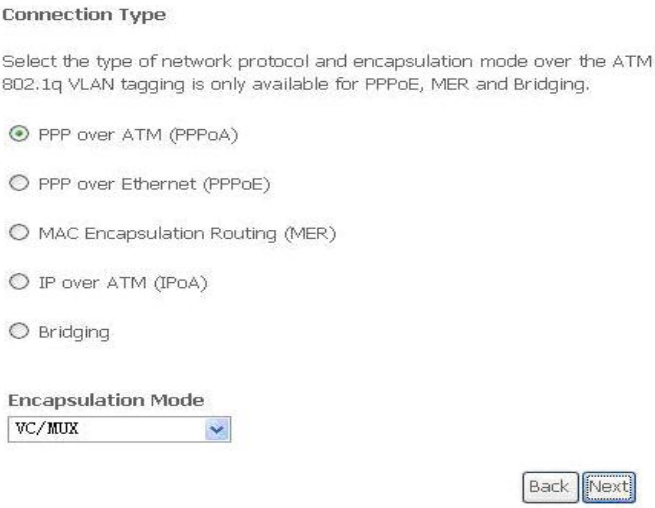

Connection Type
Select the type of network protocol and encapsulation mode over the ATM PVC that 802.1q VLAN tagging is only available for PPPoE, MER and Bridging.
PPP over ATM (PPPoA)
PPP over Ethernet (PPPoE)
MAC Encapsulation Routing (MER)
IP over ATM (IPoA)
Bridging
Encapsulation Mode
VC/MUX
Back
Next

Figure: PPP over ATM (PPPoA)

C. Click 'Next' button to enter PPP information as below page:

PPP Username and Password
PPP usually requires that you have a user name and password to establish your name and password that your ISP has provided to you.
PPP Username:
PPP Password:
Authentication Method:
AUTO
Dial on demand (with idle timeout timer)
Inactivity Timeout (minutes) [1-4320]:
0
PPP IP extension
Advanced DMZ
Non DMZ IP Address:
Non DMZ Net Mask:
Use Static IP Address
IP Address:
Retry PPP password on authentication error
Enable PPP Debug Mode
Back
Next

Figure: PPP information and others functions page

Your Internet Service Provider (ISP) should provide you with the following information:

- PPP Username
- PPP Password
- Authentication Method

You can also select another service function as below:

- Dial on demand (with idle timeout timer)
- PPP IP extension
- Use Static IP Address
- Retry PPP password on authentication error
- Enable PPP Debug Mode

D. Click ‘Next’ button to enter WAN and IGMP function information as below page:
If you want to use IGMP service on pppoa pvc, we must select ‘Enable IGMP Multicast’ box.

Figure: PPPoA IGMP and WAN service page

3.1.1.4 Internet Connection Type-PPP over Ethernet (PPPoE)

A. Setup the PVC and Qos

B. Select 'PPP over Ethernet (PPPoE)' from the 'Connection Type' box and It’s Encapsulation Type from the ' Encapsulation Mode' combo box:

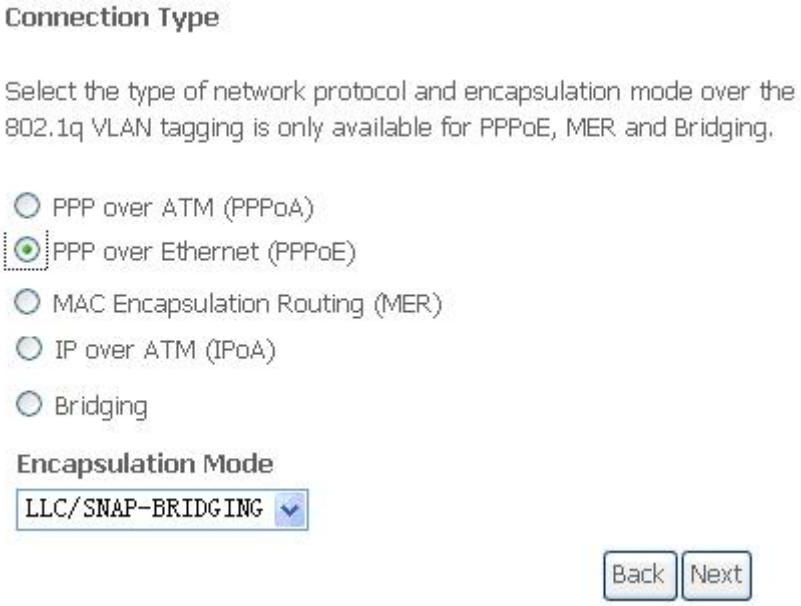

Connection Type
Select the type of network protocol and encapsulation mode over the 802.1q VLAN tagging is only available for PPPoE, MER and Bridging.
PPP over ATM (PPPoA)
PPP over Ethernet (PPPoE)
MAC Encapsulation Routing (MER)
IP over ATM (IPoA)
Bridging
Encapsulation Mode
LLC/SNAP-BRIDGING
Back
Next

Figure: PPP over Ethernet (PPPoE)

C. Click ‘Next’ button to enter PPP information as below page:

PPP Username and Password
PPP usually requires that you have a user name and password to establish your name and password that your ISP has provided to you.
PPP Username:
PPP Password:
Authentication Method:
AUTO
Dial on demand (with idle timeout timer)
Inactivity Timeout (minutes) [1-4320]:
0
PPP IP extension
Advanced DMZ
Non DMZ IP Address:
Non DMZ Net Mask:
Use Static IP Address
IP Address:
Retry PPP password on authentication error
Enable PPP Debug Mode
Back
Next

Figure: PPP information and other functions page

Your Internet Service Provider (ISP) should provide you with the following information:

- PPP Username
- PPP Password
- Authentication Method

You can also select another service function as below:

- Dial on demand (with idle timeout timer)
- PPP IP extension
- Use Static IP Address
- Retry PPP password on authentication error
- Enable PPP Debug Mode

D. Click ‘Next’ button enter WAN and IGMP function information as below page:

If you want to use IGMP service on PPPoE PVC, we must select ‘Enable IGMP Multicast’ box.

Figure: PPPoE IGMP and WAN service page

3.1.1.5 Internet Connection Type-MAC Encapsulation Routing (MER)

A. Setup the PVC and Qos

B. Select 'MAC Encapsulation Routing (MER)' from the 'Connection Type' box and It’s Encapsulation Type from the ' Encapsulation Mode' combo box:

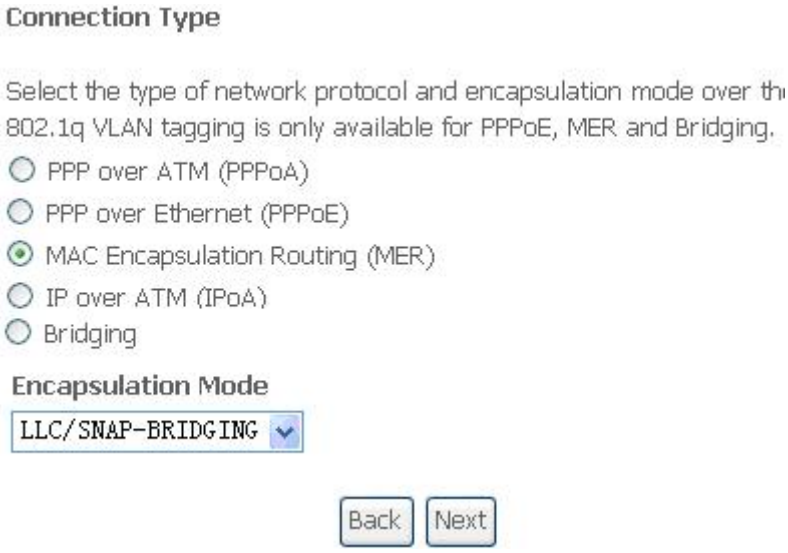


Figure : MAC Encapsulation Routing (MER)

C. Click ‘Next’ button to enter WAN IP information as below page:

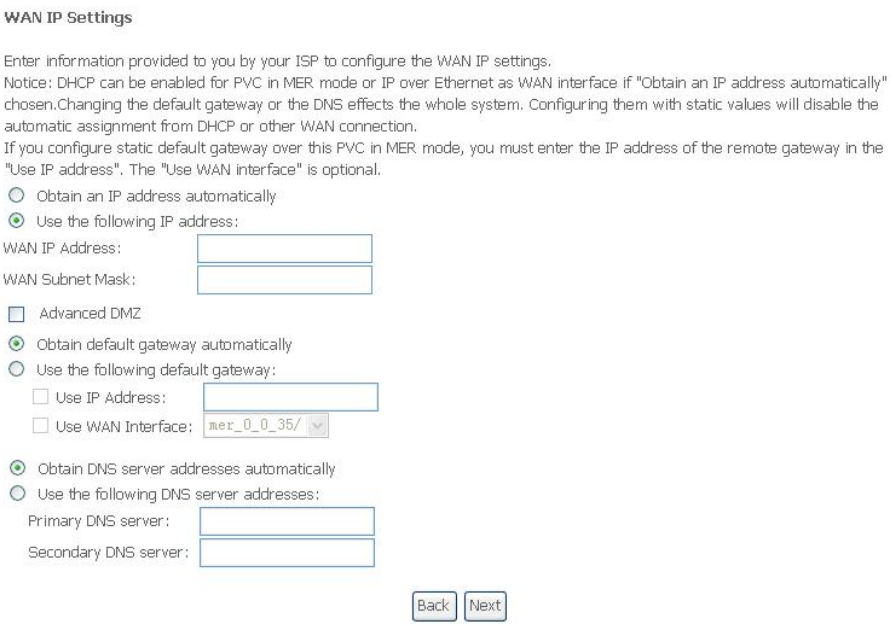

WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: DHCP can be enabled for PVC in MER mode or IP over Ethernet as WAN interface if "Obtain an IP address automatically" chosen.Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.
If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address". The "Use WAN interface" is optional.
Obtain an IP address automatically
Use the following IP address:
WAN IP Address:
WAN Subnet Mask:
Advanced DMZ
Obtain default gateway automatically
Use the following default gateway:
Use IP Address:
Use WAN Interface:
mer_0_0_35/
Obtain DNS server addresses automatically
Use the following DNS server addresses:
Primary DNS server:
Secondary DNS server:
Back
Next

Figure: WAN IP config page

Your Internet Service Provider (ISP) should provide you with the following
You can also select another service function as below:

- Obtain an IP address automatically (use DHCP to obtain WAN IP)
- Use the following IP address (use static WAN IP)
- Advanced DMZ
- Obtain default gateway automatically (use dhcp to obtain gateway IP)
- Use the following default gateway (use static gateway IP)
- Obtain DNS server addresses automatically (use dhcp to obtain DNS server IP)
- Use the following DNS server addresses (use static DNS server IP)

D. Click ‘Next’ button to enter WAN and IGMP function information as below page:

If you want to use IGMP service on MER pvc, we must select ‘Enable IGMP Multicast’ box.
In MER mode, There are some functions:

- Enable NAT
- Enable Fullcone NAT
- Enable Firewall

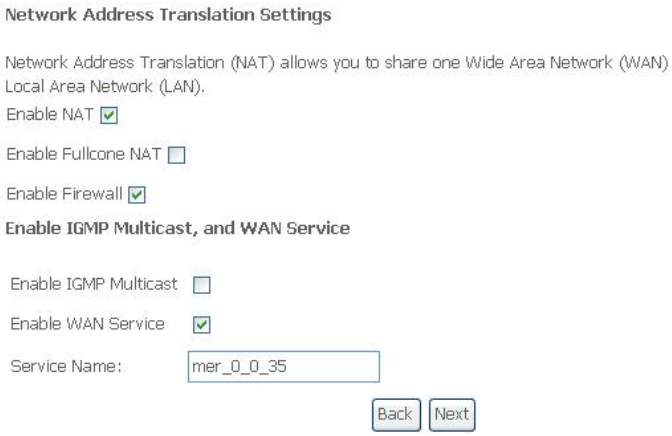


Figure: MER IGMP and WAN service page

3.1.1.6 Internet Connection Type-IP over ATM (IPoA)

A. Setup the PVC and Qos

B. Select 'IP over ATM (IPoA)' from the 'Connection Type' box and It's Encapsulation Type from the ' Encapsulation Mode' combo box:

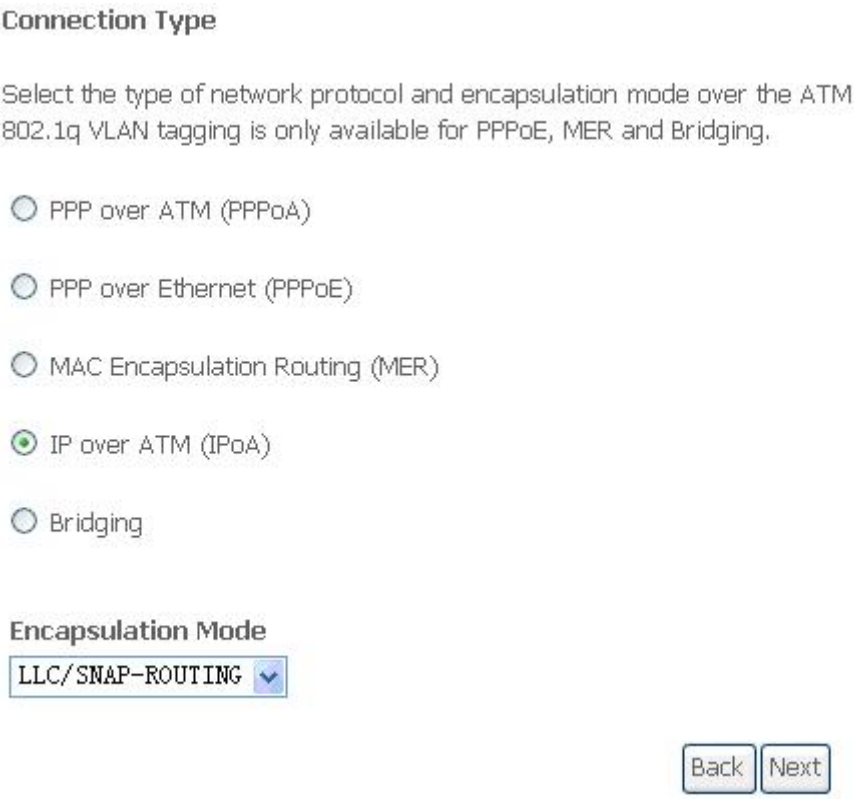

Connection Type
Select the type of network protocol and encapsulation mode over the ATM PVC tha
802.1q VLAN tagging is only available for PPPoE, MER and Bridging.
PPP over ATM (PPPoA)
PPP over Ethernet (PPPoE)
MAC Encapsulation Routing (MER)
IP over ATM (IPoA)
Bridging
Encapsulation Mode
LLC/SNAP-ROUTING
Back
Next

Figure: IP over ATM (IPoA)

C. Click 'Next' button to enter WAN IP information as below page:

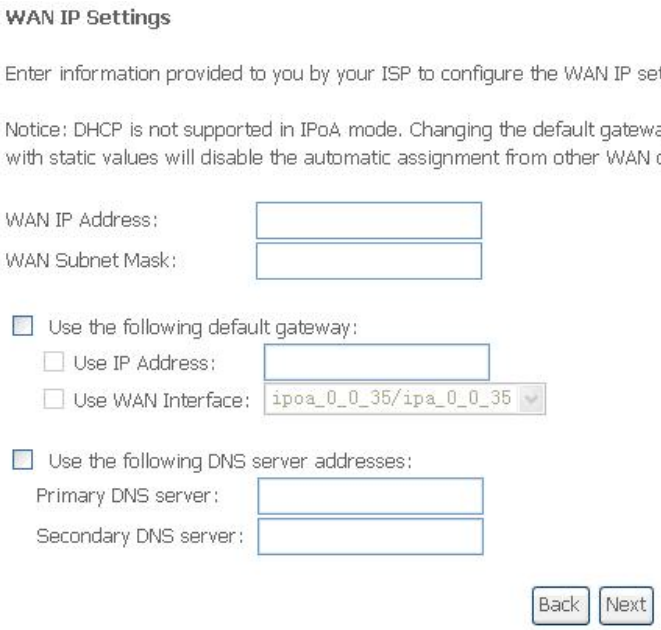

WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: DHCP is not supported in IPoA mode. Changing the default gateway or the DNS effects the whole system.
with static values will disable the automatic assignment from other WAN connection.
WAN IP Address:
WAN Subnet Mask:
Use the following default gateway:
Use IP Address:
Use WAN Interface:
ipoa_0_0_35/ipa_0_0_35
Use the following DNS server addresses:
Primary DNS server:
Secondary DNS server:
Back
Next

Figure: WAN IP config page

Your Internet Service Provider (ISP) should provide you with the following
You can also select another service function as below:

- Use the following IP address (static WAN IP)
- Use the following default gateway (static gateway IP)
- Use the following DNS server addresses (static DNS server IP)

D. Click ‘Next’ button to enter WAN and IGMP function information as below page:
If you want to use IGMP service on ipoa pvc, we must select ‘Enable IGMP Multicast’ box.
In IPoA mode, there are some functions:

- Enable NAT
- Enable Fullcone NAT
- Enable Firewall

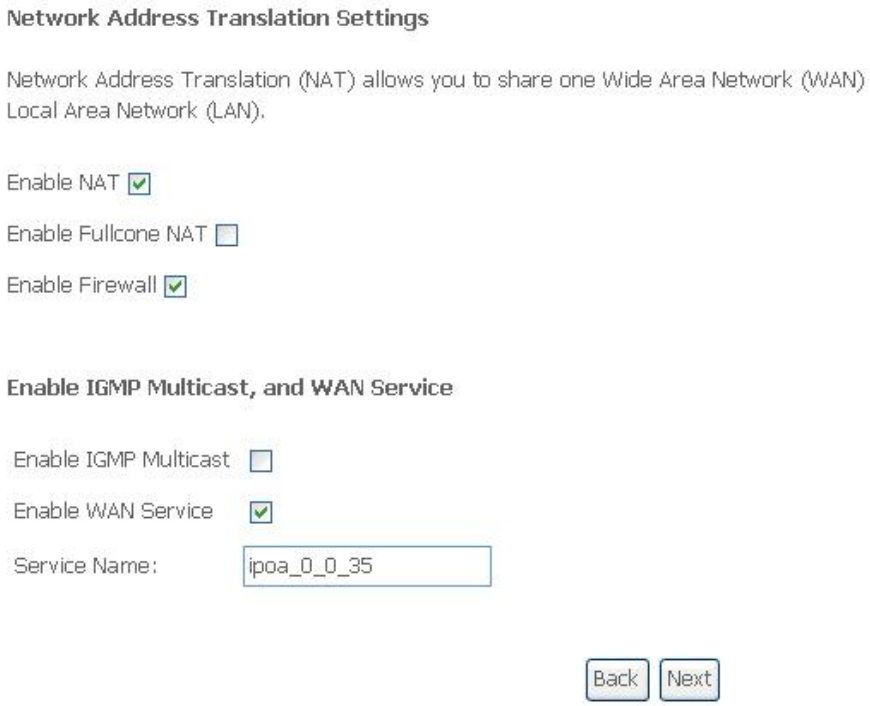


Figure: IPOA IGMP and WAN service page

3.1.1.7 Internet Connection Type-Bridging

A. Setup the PVC and Qos

B. Select 'Bridge' from the 'Connection Type' box and It's Encapsulation Type from the ' Encapsulation Mode' combo box:

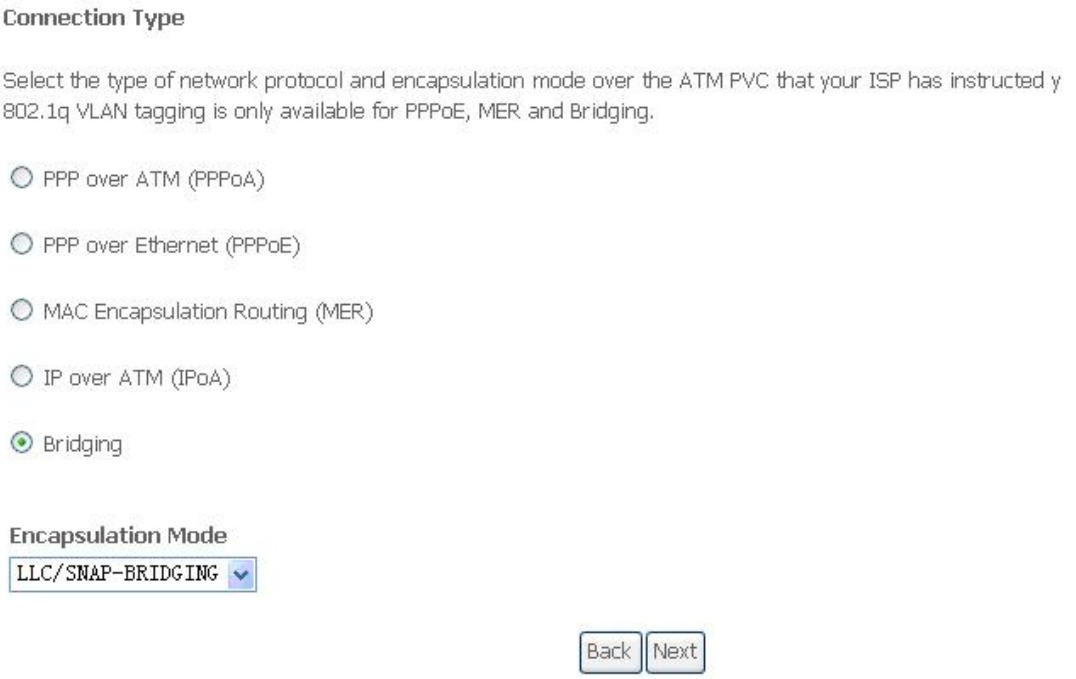

Connection Type
Select the type of network protocol and encapsulation mode over the ATM PVC that your ISP has instructed y
802.1q VLAN tagging is only available for PPPoE, MER and Bridging.
PPP over ATM (PPPoA)
PPP over Ethernet (PPPoE)
MAC Encapsulation Routing (MER)
IP over ATM (IPoA)
Bridging
Encapsulation Mode
LLC/SNAP-BRIDGING
Back
Next

Figure: Bridging

C. Click 'Next' button to enter WAN function information as below page:

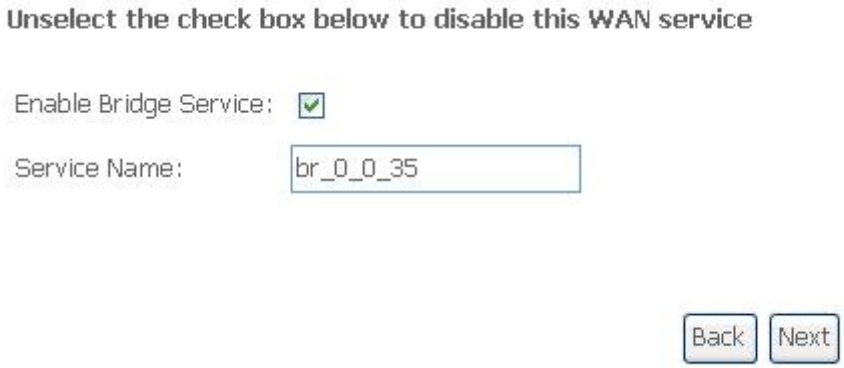


Figure: Bridging service page

3.1.2 LAN Interface Setup

In LAN interface setup page, you can modify your default LAN IP and DHCP Server settings. The Default LAN IP is **192.168.1.1** and DHCP is **Enable**.

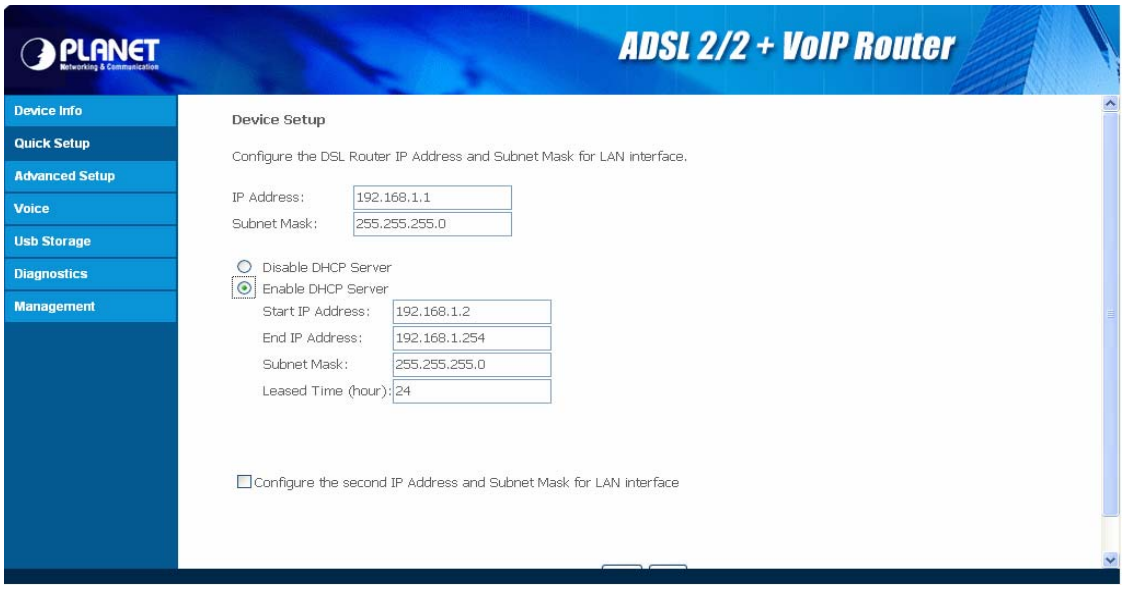


Figure: LAN Interface Setup

Configuring the DHCP server

The Router has a DHCP server for which the factory setting is active. Consequently, the IP addresses of the PCs are automatically assigned by the DSL Router.

Note:

- If the DHCP server for the DSL Router is activated, you can configure the network setting on the PC so that the option Obtain an IP address automatically is set up. Further information about this can be found in the section entitled
- If you deactivate the DHCP server, you will have to assign a static IP address for the PCs that use the network settings

➢ To activate the DHCP server, select ‘Enable’.

➢ If the DHCP server is active, you can define a Lease time. The Lease time determines the period for which the PCs retain the IP addresses assigned to them without changing them.

Note:

If you select Never expires, the IP addresses are never changed. Activate this option if you want to make NAT or firewall settings using the IP addresses of the PCs; otherwise you have to assign static IP addresses to these PCs.

3.1.3 WAN Setup Summary

When In WAN setup summary phase, the property of the PVC added can view:

- VPI/VCI
- Connection Type:
- Service Name:
- Service Category:
- IP Address:
- Service State:
- NAT
- Firewall
- IGMP
- QOS

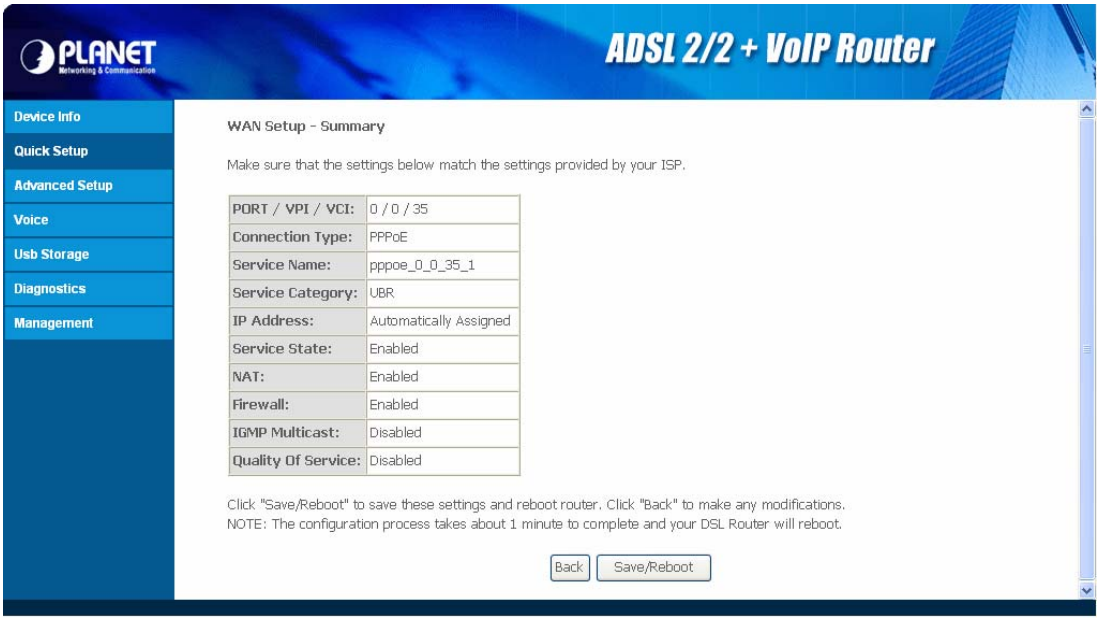

PLANET
ADSL 2/2 + VoIP Router
Device Info
Quick Setup
Advanced Setup
Voice
Usb Storage
Diagnostics
Management
WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
PORT / VPI / VCI: 0 / 0 / 35
Connection Type: PPPoE
Service Name: pppoe_0_0_35_1
Service Category: UBR
IP Address: Automatically Assigned
Service State: Enabled
NAT: Enabled
Firewall: Enabled
IGMP Multicast: Disabled
Quality Of Service: Disabled
Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.
Back
Save/Reboot

Figure: WAN setup summary

Click “Save/Reboot” to save these settings. And you can click “Back” to make any modifications. After you click “Save/Reboot”, it shows the following message.

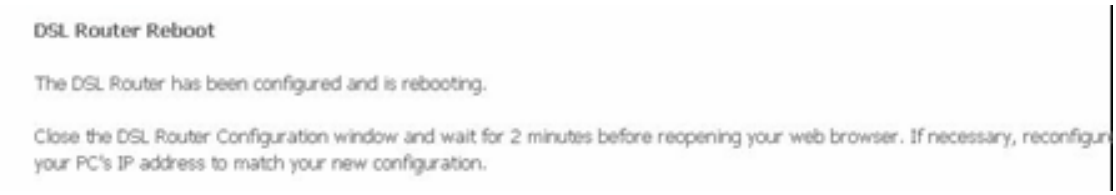

DSL Router Reboot
The DSL Router has been configured and is rebooting.
Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigur
your PC's IP address to match your new configuration.

Figure: DSL Router Reboot

NOTE: You need to reboot to activate this WAN interface and further configure services over this interface，and it will take about two minutes to done with it.

3.1.4 Quick Setup Completed

DSL router does not require further configuration in order to start working. After the setup described in this chapter, you can immediately start using your gateway to:

- Share a broadband connection among multiple users (HTTP, FTP, Telnet, and NetMeeting) and between all of the computers connected to your home network.
- Build a home network by connecting additional PCs and network devices to the gateway.
- Control network parameters, including DHCP, DNS and WAN settings.
- View network status, traffic statistics, system log and more.
- Allow access from the Internet to games and other services provided by computers in the home network.
- Prohibit computers in the home network from accessing selected services on the Internet.
- Block access to specific Internet Web sites from your home network. To learn about how to configure your Firewall security parameters, please refer to section 7.3. If you wish to apply corporate-grade security to your network, please refer to section 7.3.11.

If your gateway is equipped with multiple LAN ports, you can connect additional devices directly to the gateway. Otherwise, connect a hub or switch to the LAN port, to which you can connect additional devices. In both cases, configure newly connected devices to automatically obtain IP address as described above.

3.2 DSL Router Device information

Click “Device Info”, It should view the information as below:

- Summary
- WAN
- Statistics
- Route
- ARP
- DHCP

3.2.1 Summary of Device information

This interface contains the following information:

- Board ID:
- Software Version:
- Bootloader (CFE) Version:
- Upstream Line Rate
- Downstream Line Rate
- LAN IP Address: The management IP address
- Default Gateway: No gateway in a pure bridging mode; under other modes such as PPPOE/PPPOA, it is the address of the uplink equipment.
- DNS Server address: Obtained from the uplink equipment in PPPOE/PPPOA mode; No DNS Server address in a pure bridging mode; or input them manually.

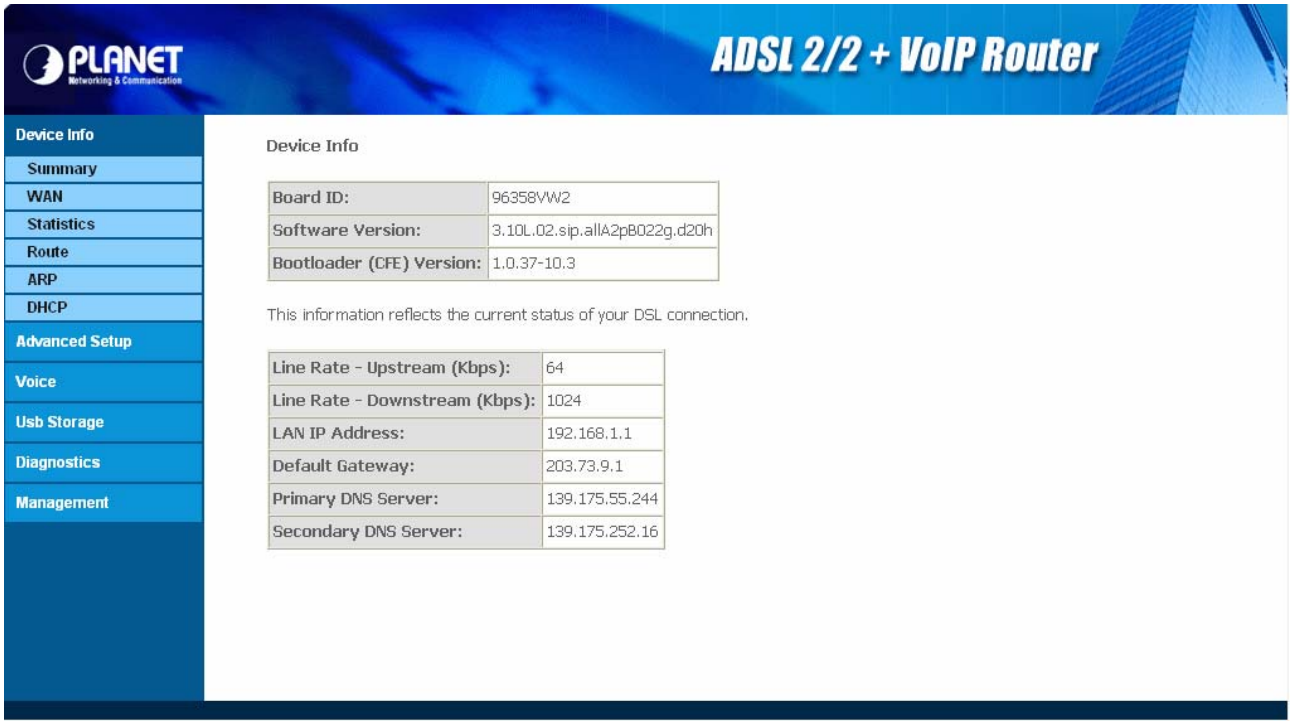


Figure: summary of Device information

3.2.2 WAN Interface information

Click “WAN” to show the following interface, depend on the selected connection mode, the Summary screen shows the status and also the connect or disconnect button.

This interface contains the following informations of every WAN connection:

- VPI/VCI
- VLAN
- Connection ID
- Category
- Service
- Interface
- Protocol
- IGMP
- Qos
- State
- Status
- IP address

Figure: WAN interface info

3.2.3 Statistics

In this page, It includes four parts information:

- Statistics of LAN
- Statistics of WAN
- Statistics of ATM
- Statistics of ADSL

3.2.3.1 Statistics of LAN

Click “Statistics”-->”LAN” to show the following interface. You can query information on packets recevied at the Ethernet. Click “Reset Statistics” to return the values to zero and recount them.

You can view the info as below:

- Interface
- Received

  Bytes: Bytes of Received

  Pkts: Packets of Received

  Errs: Errors packets of Received

  Drops: Drops packets of Received
- Transmitted

  Bytes: Bytes of Received

  Pkts: Packets of Received

  Errs: Errors packets of Received

  Drops: Drops packets of Received

Figure: Statistics of LAN

3.2.3.2 Statistics of WAN

Click “Statistics”-->”WAN” to show the following interface. You can query information on packets recevied at the WAN interfaces. Click “Reset Statistics” to return the values to zero and recount them.

Informations as below:

- Service
- VPI/VCI
- Protocol
- Interface
- Received

  Bytes: Bytes of Received

  Pkts: Packets of Received

  Errs: Errors packets of Received

  Drops: Drops packets of Received
- Transmitted

  Bytes: Bytes of Received

  Pkts: Packets of Received

  Errs: Errors packets of Received

  Drops: Drops packets of Received

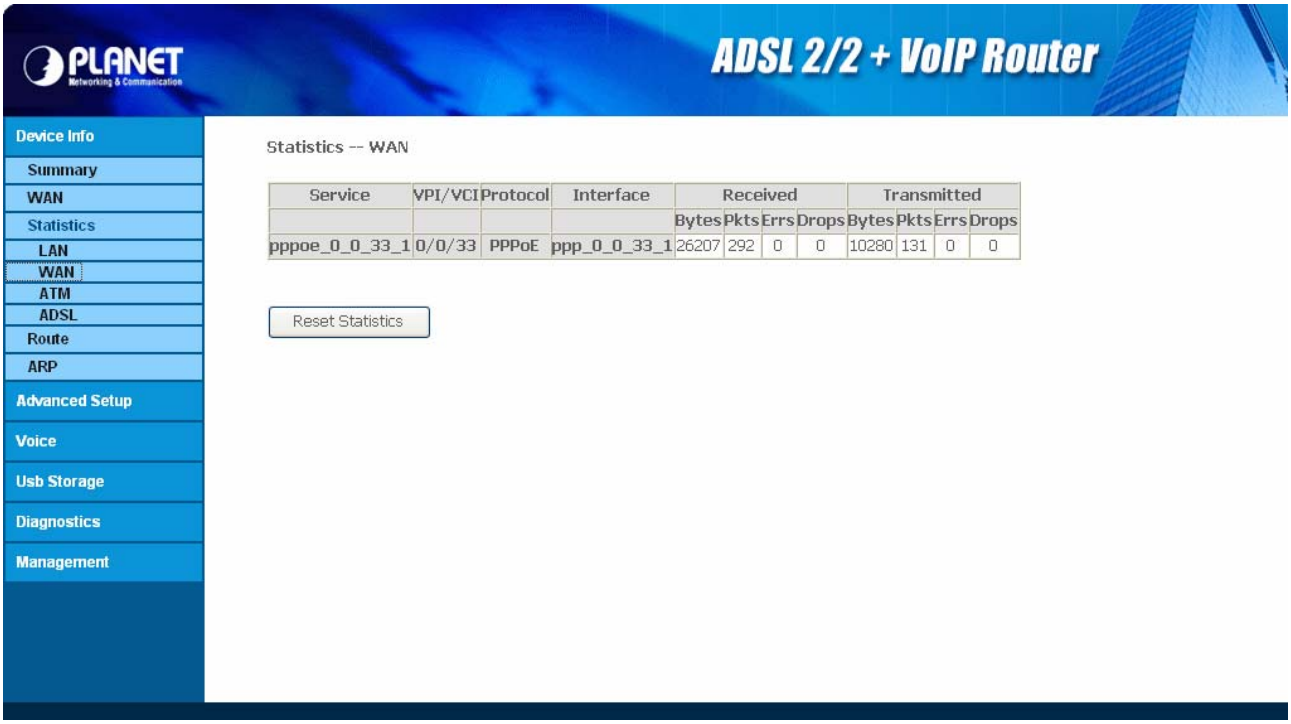


Figure: Statistics of WAN

3.2.3.3 Statistics of ATM

Click “Statistics”-->”ATM” to show the following interface. You can query information on packets recevied at the ATM interfaces. Click “Reset” to return the values to zero and recount them.

There are three part info:

- ATM Interface Statistics:
  In Octets
  Out Octets
  In Errors
  In Unknown
  In Hec Errors
  In Invalid Vpi Vci Errors
  In Port Not Enable Errors
  In PTI Errors
  In Idle Cells In Circuit Type Errors
  In OAM RM CRC Errors
  In GFC Errors

- AAL5 Interface Statistics:
  In Octets
  Out Octets
  In Ucast Pkts
  Out Ucast Pkts
  In Errors
  Out Errors
  In Discards
  Out Discards

- AAL5 VCC Statistics:
  VPI/VCI
  CRC Errors
  SAR Timeouts
  Oversized SDUs
  Short Packet Errors
  Length Errors

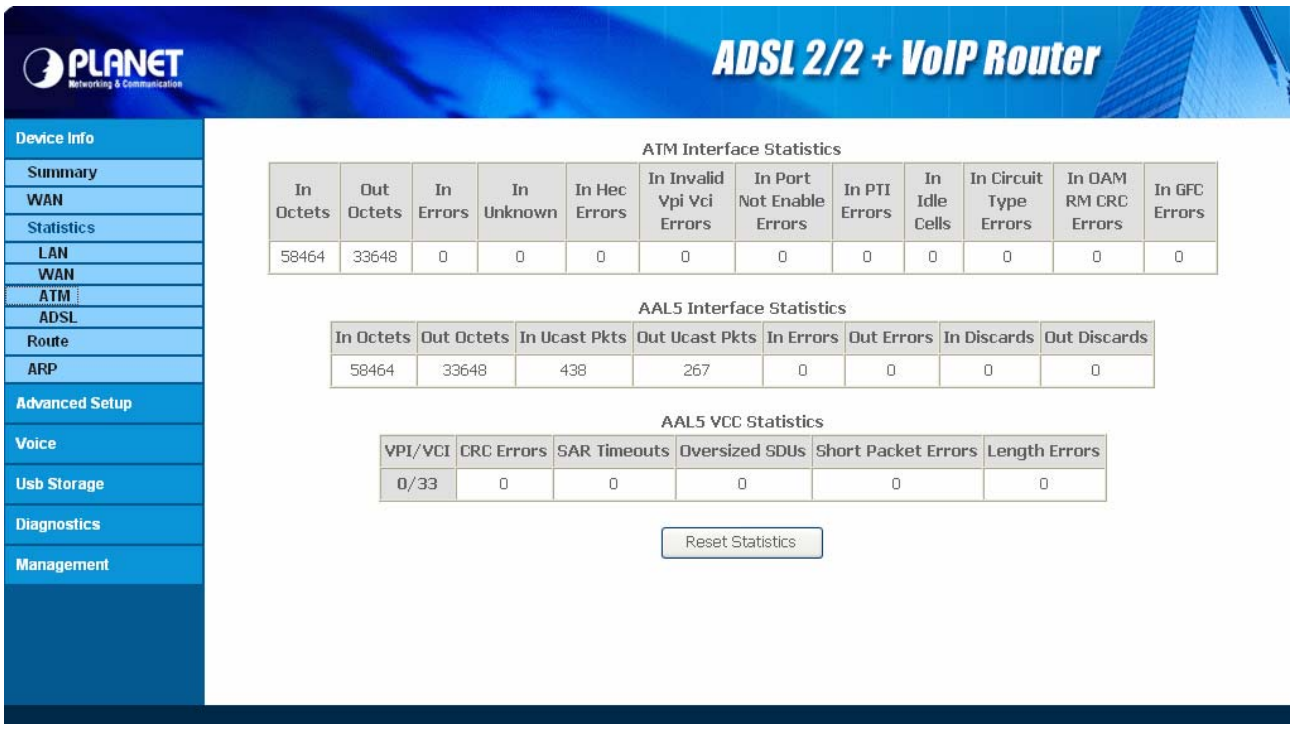
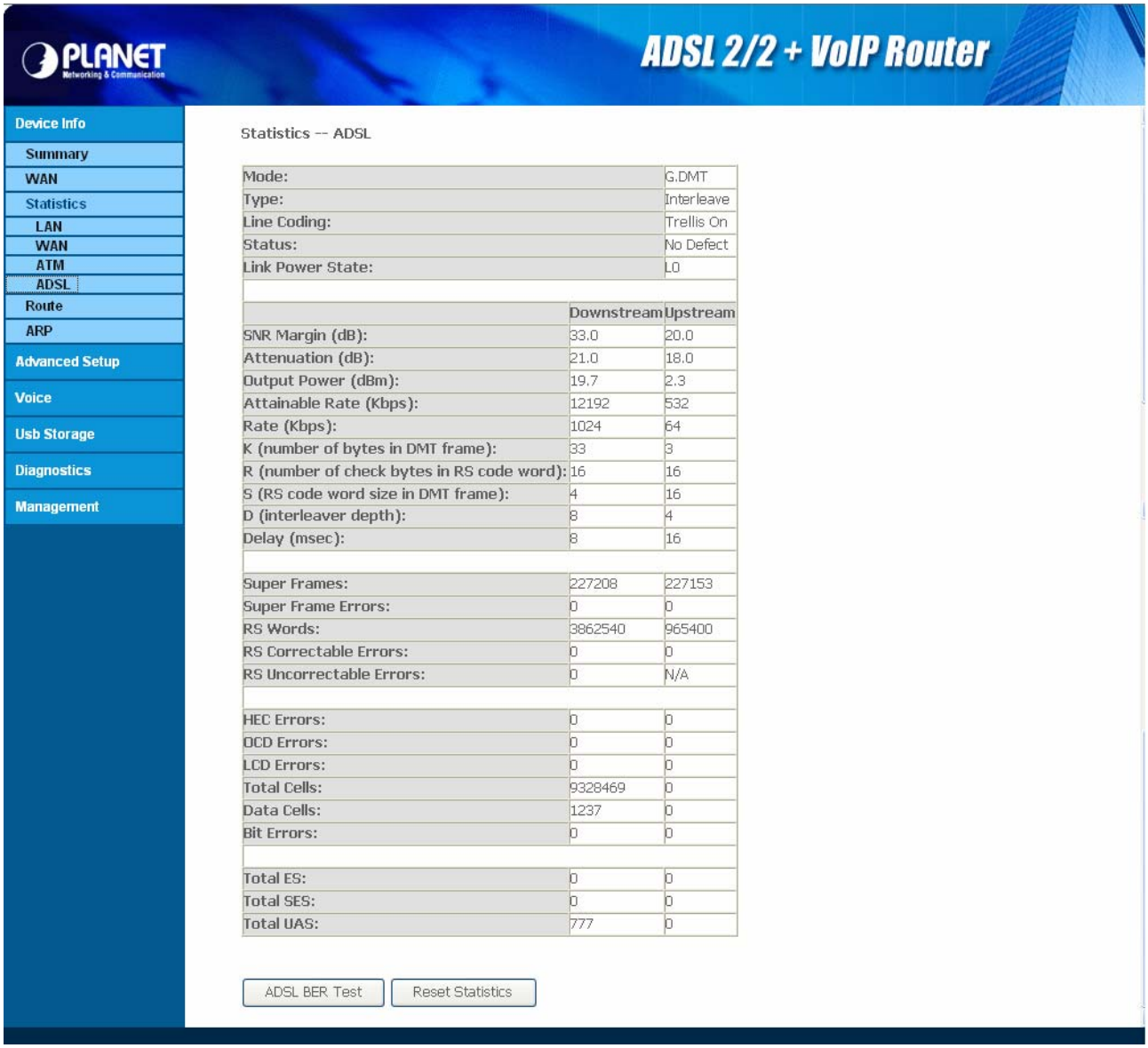


Figure: Statistics of ATM

3.2.3.4 Statistics of ADSL

Click “Statistics”-->”ADSL” to show the following interface.

If the DSL line is activated, the following window will show.



Mode:		G.DMT
Type:		Interleave
Line Coding:		Trellis On
Status:		No Defect
Link Power State:		L0
	Downstream	Upstream
SNR Margin (dB):	33.0	20.0
Attenuation (dB):	21.0	18.0
Output Power (dBm):	19.7	2.3
Attainable Rate (Kbps):	12192	532
Rate (Kbps):	1024	64
K (number of bytes in DMT frame):	33	3
R (number of check bytes in RS code word):	16	16
S (RS code word size in DMT frame):	4	16
D (interleaver depth):	8	4
Delay (msec):	8	16
Super Frames:	227208	227153
Super Frame Errors:	0	0
RS Words:	3862540	965400
RS Correctable Errors:	0	0
RS Uncorrectable Errors:	0	N/A
HEC Errors:	0	0
OCD Errors:	0	0
LCD Errors:	0	0
Total Cells:	9328469	0
Data Cells:	1237	0
Bit Errors:	0	0
Total ES:	0	0
Total SES:	0	0
Total UAS:	777	0

Figure: Statistics of ADSL

You will see the following information pertinent to the ADSL line in the page:

- Mode: G.DMT/G.LITE/T1.413/ADSL 2+/ADSL 2/READSL2
- Line Coding: Trallis on, etc.
- Status: Link Down, No Defect, Training
- Link Power State: L0, L1, L2
- Rate (Kbps): Upstream Line Rate/Downstream Line Rate.

At the lower part of this interface, there is a “Reset Statistics” button. Click it to return values to zero and recount.

ADSL BER Test

Click “ADSL BER Test” to do a “Bit Error Rate” Test on the DSL line. The test interface is as follows:

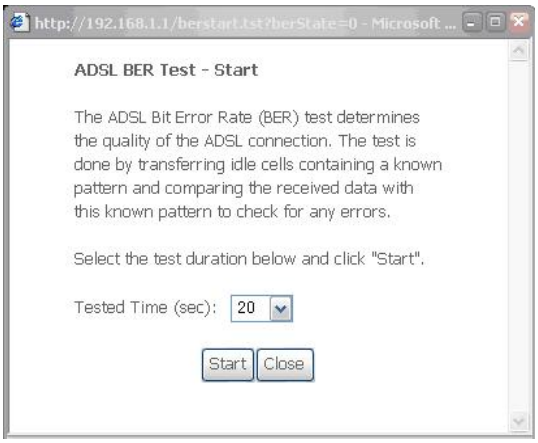

http://192.168.1.1/berstart.tst?berState=0 - Microsoft ...
ADSL BER Test - Start
The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.
Select the test duration below and click "Start".
Tested Time (sec): 20
Start
Close

Figure: ADSL BER Test

The Tested Time (sec) has the following choices: 1, 5, 10, 20, 60, 120, 180, 240, 300, and 360. Select a time and then click “Start” to pop up the following interfaces in sequence.

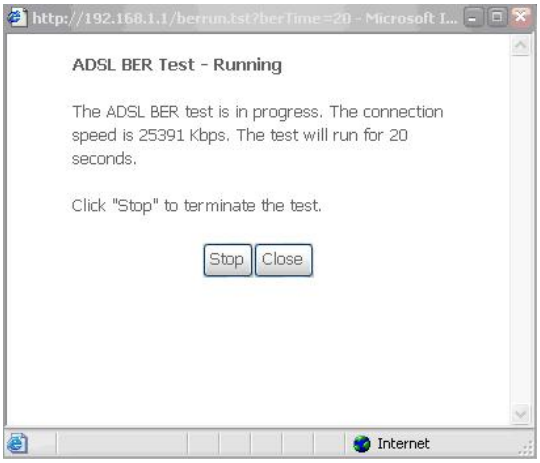

http://192.168.1.1/berrun.tst?berTime=20 - Microsoft I...
ADSL BER Test - Running
The ADSL BER test is in progress. The connection speed is 25391 Kbps. The test will run for 20 seconds.
Click "Stop" to terminate the test.
Stop
Close
Internet

Figure: ADSL BER Test Running Page

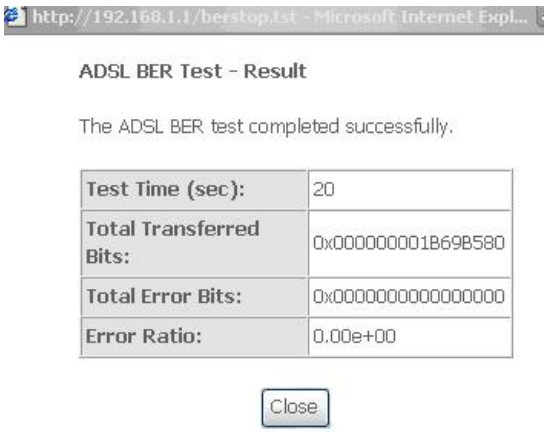

http://192.168.1.1/berstop.tst - Microsoft Internet Expl...
ADSL BER Test - Result
The ADSL BER test completed successfully.
Test Time (sec): 20
Total Transferred Bits: 0x000000001B69B580
Total Error Bits: 0x0000000000000000
Error Ratio: 0.00e+00
Close

Figure: ADSL BER Test Result

Note: If the error ratio reaches up to “e-5”, the user will not be able to access the Internet.

3.2.4 Route table information

Click “Route”. You can view the route table information,Each route item in route table has info as below:

- Destination
- Gateway
- Subnet Mask
- Flag
- Metric
- Service
- Interface

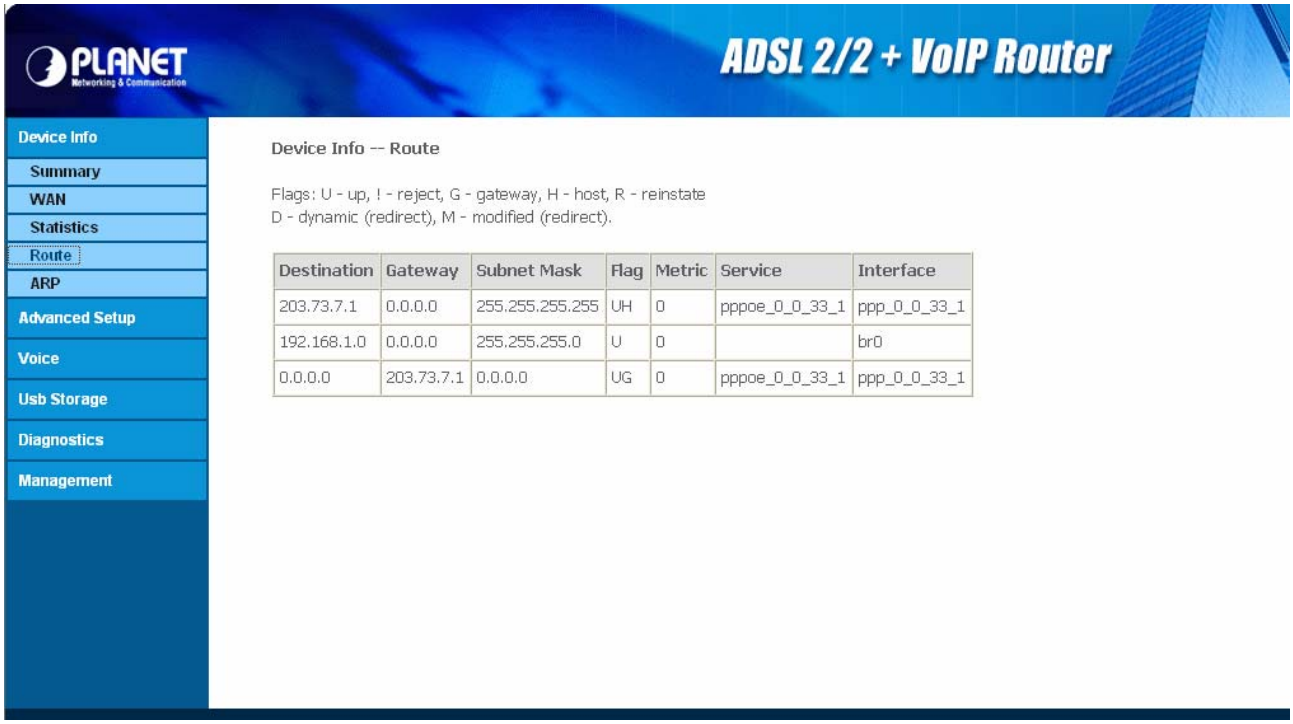


Figure: route table

3.2.5 ARP table information

Click “ARP” to show the following interface. You can query the MAC and IP addresses information of the equipment attached to the Router.

Each ARP item has information as below:

- IP address
- Flags
- HW address
- Device

Figure: ARP table

3.2.6 DHCP IP Leases information

Click “DHCP” to show the following interface. You can query the IP addresses assignment to which MAC Address in DSL router’s LAN side,Through Ethernet can obtain the IP Address from the DHCP server on DSL router.

Each Leases item include info as below:

- Hostname
- MAC Address
- IP Address
- Expires In: How many times the Device Leases the IP Address for the MAC Address

Figure: DHCP Leases List

3.3 Advanced Setup

Click “Advanced Setup” to enter the advanced system setup interface.there many items as below:

- WAN : Wide area network interface,
- LAN : Local area network interface
- NAT : Network Address Translate
- Security
- Quality of Service
- Routing
- DNS
- DSL
- Print Server
- Port Papping
- IPSec
- Certificate

Advance Setup is DSL Router’s config center,

3.3.1 WAN CONFIGRATION

Click ”Advance Setup”→ “WAN” , there maybe two circumstances appears.
In this Interface you can do:

- Add
- Edit
- Remove
- Save/Reboot

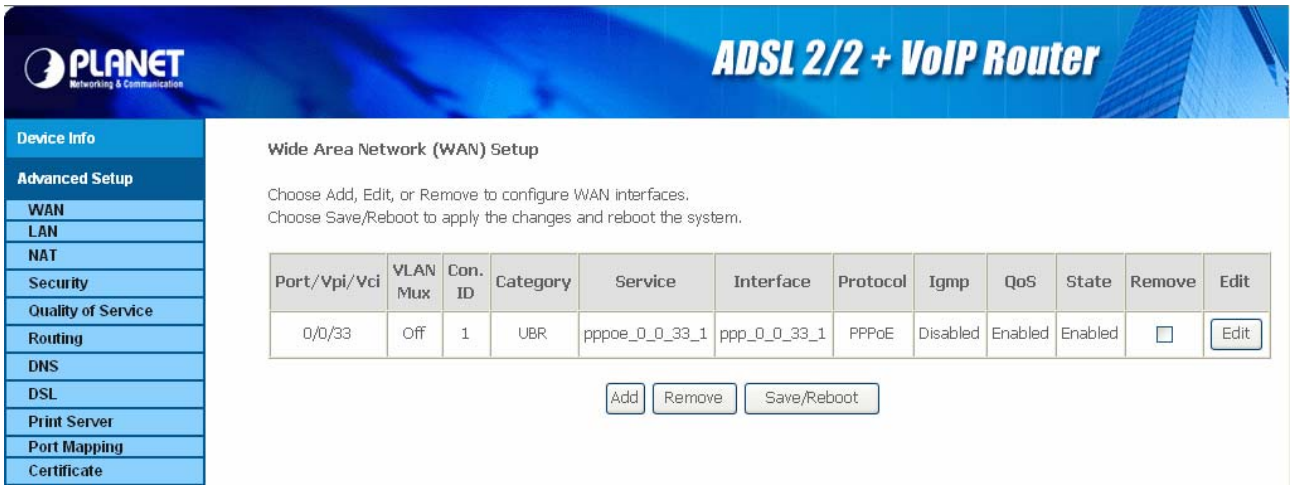


Figure: WAN Config

Select “Add”, then it will turn into the following configure screen.

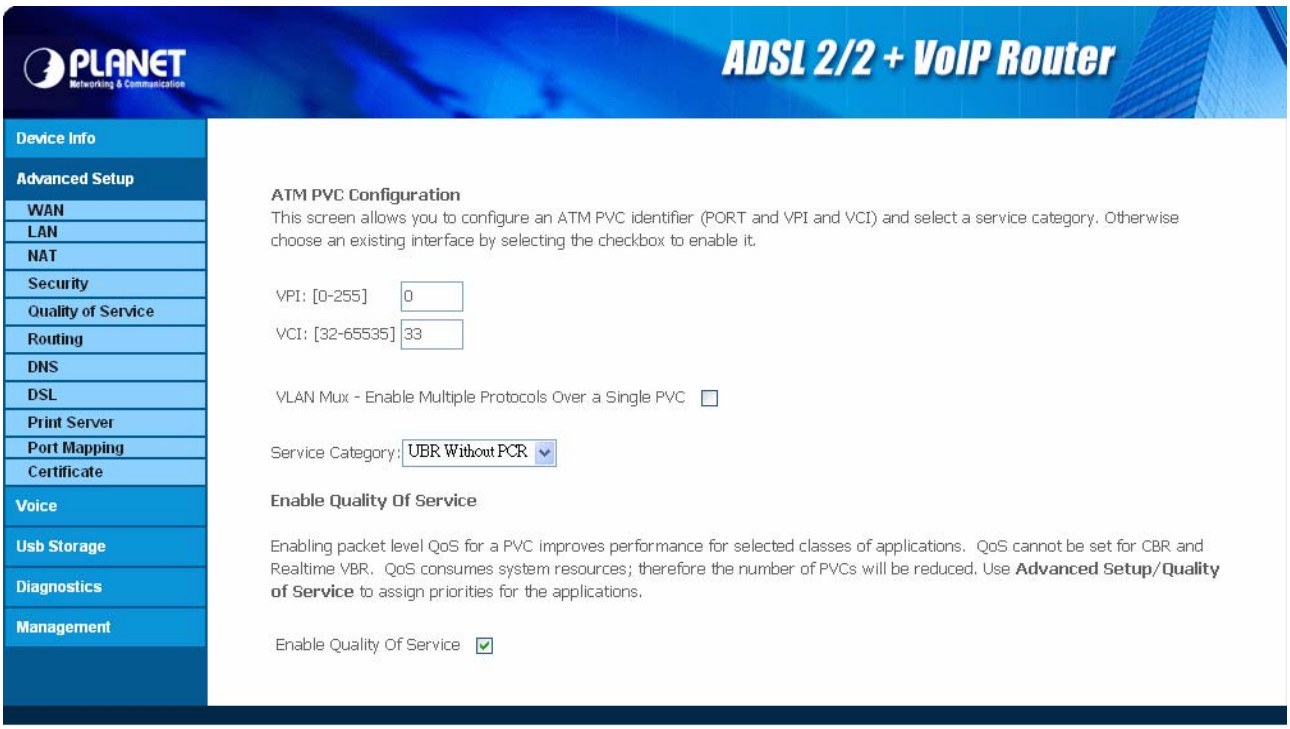

PLANET
ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
DNS
DSL
Print Server
Port Mapping
Certificate
Voice
Usb Storage
Diagnostics
Management
ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (PORT and VPI and VCI) and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.
VPI: [0-255] 0
VCI: [32-65535] 33
VLAN Mux - Enable Multiple Protocols Over a Single PVC
Service Category: UBR Without PCR
Enable Quality Of Service
Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Service to assign priorities for the applications.
Enable Quality Of Service

Figure: PVC and Qos config page

Look at this screen, is it familiar with us? Yes!!! It is the same as "**Quick Setup**", to learn more about the configuration, please turn to the page 17.

If we have configured the modem, click "WAN" will turn into the following interface:

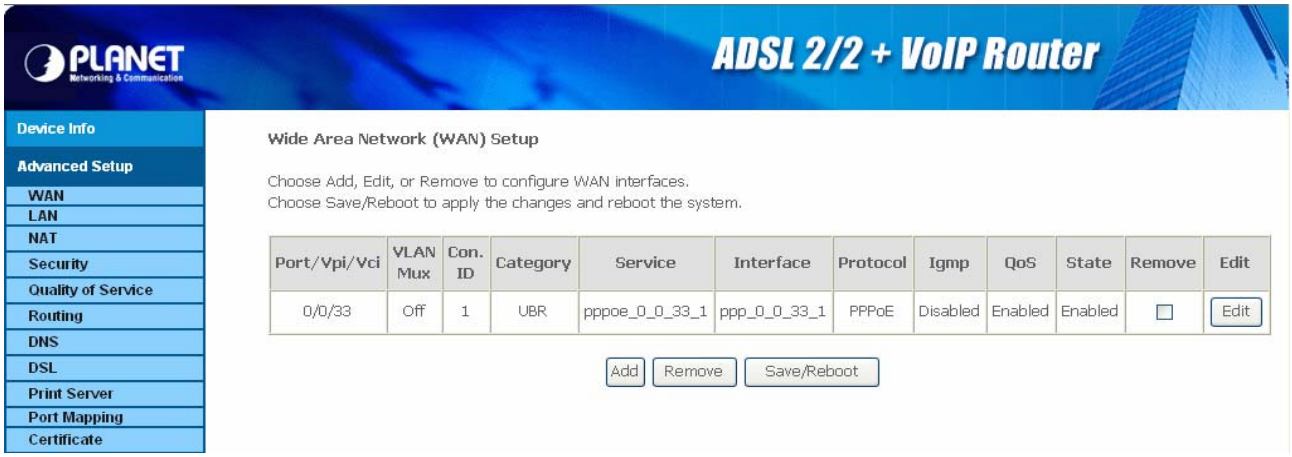


Figure: PPPoE Config

1. Select "Edit", you can modify the existent PVC's parameter.
2. Select "Add", you can add a more one ATM PVC.
3. Choose "Remove", you can delete the PVC (don't forget select the "Remove check box).
4. Select "Save/Reboot", Choose "Save/Reboot" to apply the changes and reboot the system.

Note: After a PVC is deleted or modified, the system must be rebooted, or the modification will not be effective.

Now we only show you how to add PVC.

3.3.1.1 Add PPPoE PVC

Click “Add” to add a certain piece of PVC. The following descriptions are given by an example of adding “PVC 8/35” (PPPOE mode).

1. Click “Add” to turn into the following interface. In this interface, you can modify VPI/VCI, service categories and Qos.

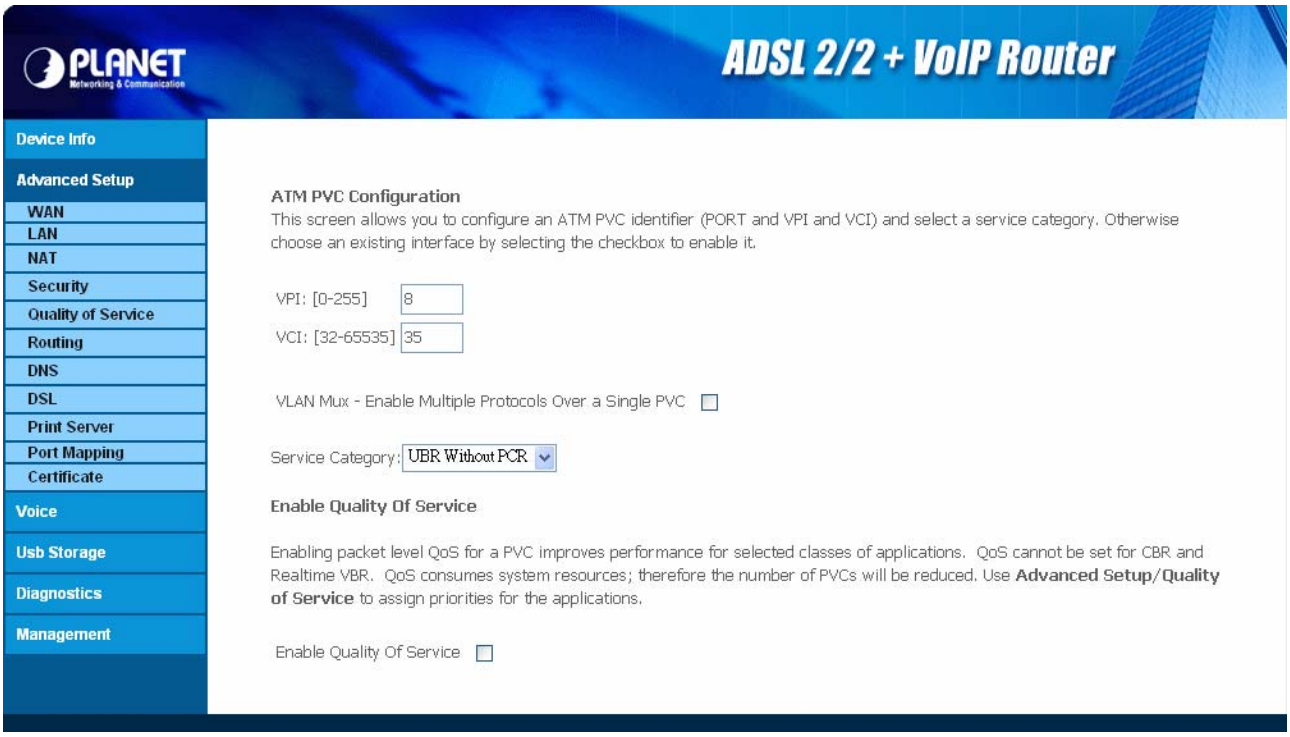

PLANET
Networking & Communication
ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
DNS
DSL
Print Server
Port Mapping
Certificate
Voice
Usb Storage
Diagnostics
Management
ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (PORT and VPI and VCI) and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.
VPI: [0-255] 8
VCI: [32-65535] 35
VLAN Mux - Enable Multiple Protocols Over a Single PVC
Service Category: UBR Without PCR
Enable Quality Of Service
Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Service to assign priorities for the applications.
Enable Quality Of Service

Figure: PVC and Qos config page

- **VPI (Virtual Path Identifier)**: The virtual path between two points in an ATM network, and its valid value is from 0 to 255.
- **VCI (Virtual Channel Identifier)**: The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols).
- **Service Category:** UBR Without PCR/UBR With PCR/CBR/Non Realtime VBR/Realtime VBR.
- **Enable Quality Of Service:** enable/disable.

In this example, PVC 8/35 is required to modify, so service category and QoS will remain default values. In actual applications, you can modify them depending on your practices.

After proper modifications, click “Next” to show the following interface.

2. In this interface, you can modify Internet Connection Type and Encapsulation Type.

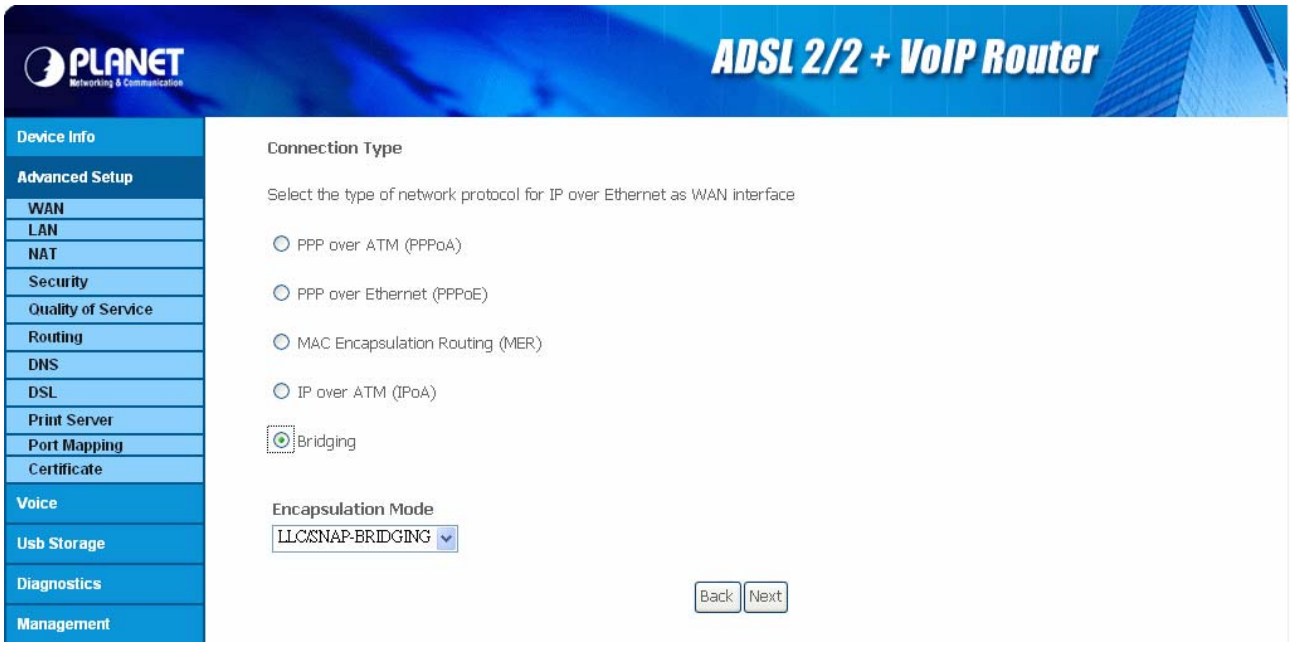


Figure: Internet Connection Type and Encapsulation Type page

Change the connection type of PVC 8/35 to “PPP over ATM (PPPoE)”.

Select “PPP over ATM (PPPoE)”, and “LLC/SNAP-BRIDGING” (depending on the uplink equipment, generally “LLC/SNAP-BRIDGING”) as “Encapsulation Mode”.

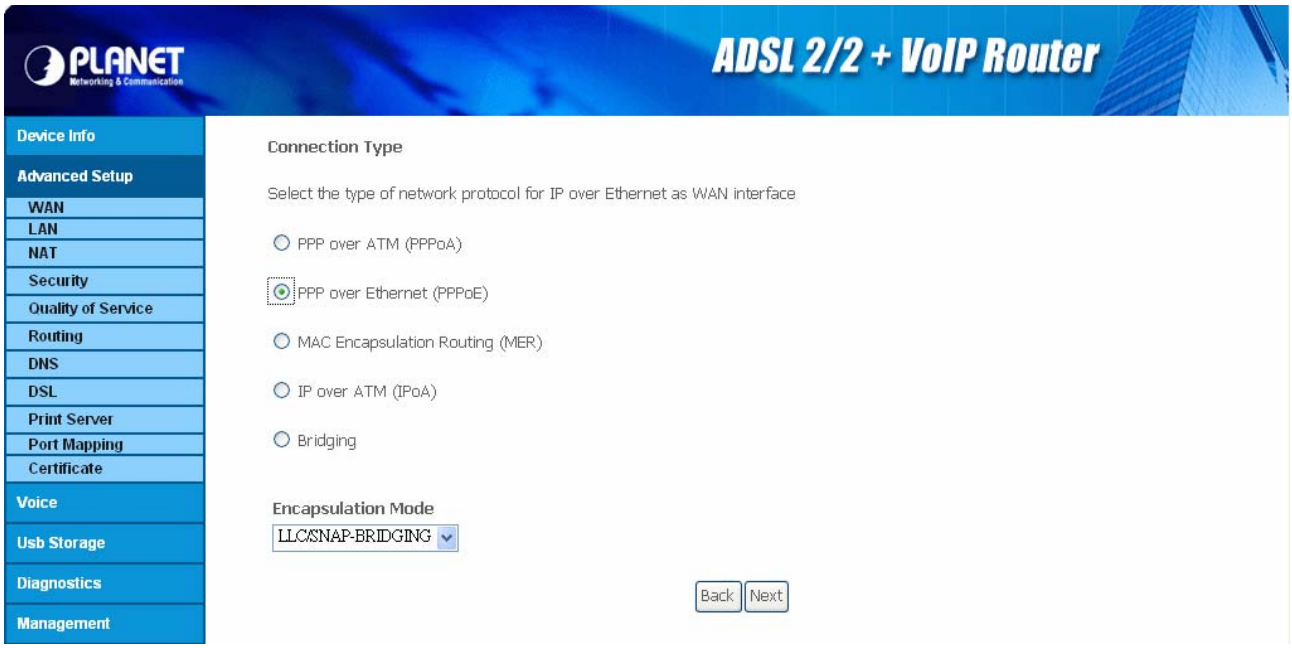


Figure: PPP over Ethernet (PPPoE)

Enable 802.1q: If enable it, input the 802.1q VLAN tag value. Note that 802.1q VLAN tagging is only available for PPPoE, MER and Bridge.

Click “Next” to show the following interface.

3. In this interface, you can modify the PPP Username, PPP Password, Authentication Method and so on.

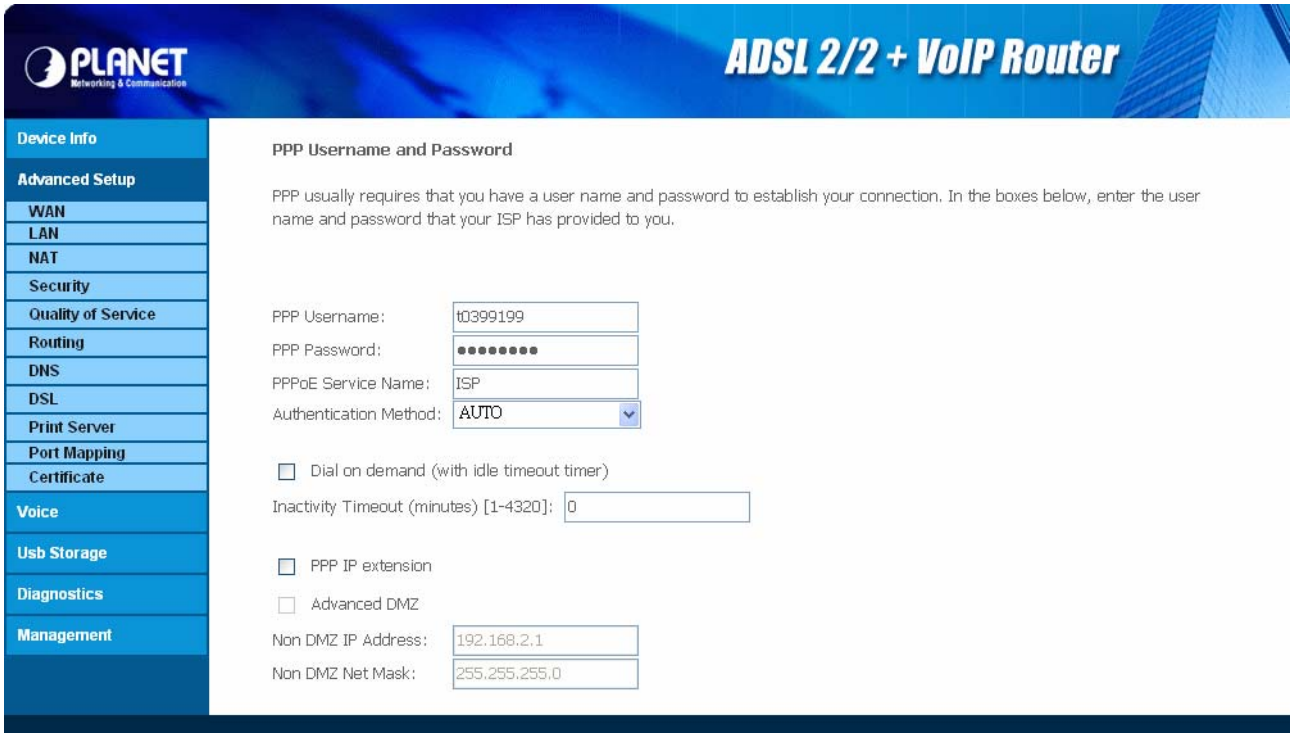


Figure: PPP information and others function page

PPP Username: the correct user name that your ISP has provided to you.

PPP Password: the correct password that your ISP has provided to you.

PPPoE Service Name: If your ISP provided it to you, please input it. Unless don't input anything.

Authentication Method: AUTO, PAP, CHAP, MSCHAP. Usually select AUTO will be OK.

Dial on demand (with idle timeout timer): If enable it, you need to input the idle timeout time. Within the preset minutes, if the MODEM doesn't detect the flow of the user continuously, the MODEM will automatically disconnect the PPPOE connection. Once it detects the flow (like access to a webpage), the MODEM will restart the PPPOE dial up.

If disable it, the MODEM will perform PPPOE dial-up all the time. Unless the MODEM is powered off and DSLAM or uplink equipment are abnormal, the PPPOE connnection will not broken.

PPP IP extension: After "PPP IP extension" is enabled, the WAN IP address obtained by the MODEM through built-in dial-up can be directly assigned to the PC being attached with the MODEM (at this time, the MODEM has only one PC). From the view of the PC user, this is even with that the PC dials up to obtain an IP addres. But actually, the dial-up is done by the MODEM.

If disable it, the MODEM obtain the WAN IP address itself.

Advanced DMZ: This is the virtual server configuration option. The DMZ Host feature allows one local computer to be exposed to the internet, to be this feature,the other computer can easily enter the DMZ Host, and a DMZ host is not protected by the firewall and may be vulnerable to attack. Designating a DMZ host may also put other computers in the home

network at risk. When designating a DMZ host, you must consider the security implications and protect it if necessary.

a. If you want to setup DMZ Host, you should enable the “PPP IP extension” at first;
b. **Non DMZ IP Address:** The DMZ Host IP Address, you can modify it by hand;
c. **Non DMZ Net Mask:** The DMZ Host Subnet Mask, it is build upon the DMZ Host IP Address.
d. **Use Static IP Address:** If disabled it, the MODEM through PPPOE dial-up, to obtain an IP address assigned by an uplink equipment such as BRAS.

If enable it, the MODEM use this IP as the WAN IP address.

After input the PPP Username and PPP Password, click “Next” to show the following interface.

4. In this interface, you can modify the Service name and enable/disable the IGMP Multicast, WAN Service.

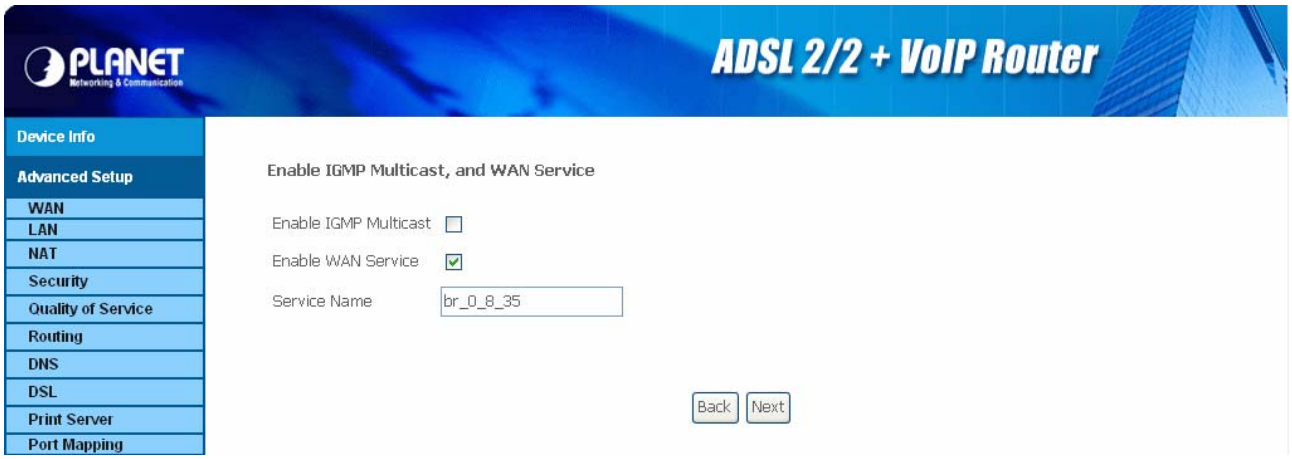


Figure: PPPoE IGMP and WAN service page

IGMP Multicast: IGMP proxy. For example, if you need PPPoE mode support IPTV, please enable it.

WAN Service: Please enable it, unless you don’t need to active the PVC.

Click “Next” to show the following interface.

5. In this interface, it show the all configuration. You can see some default values: NAT enable, Firewall enable.

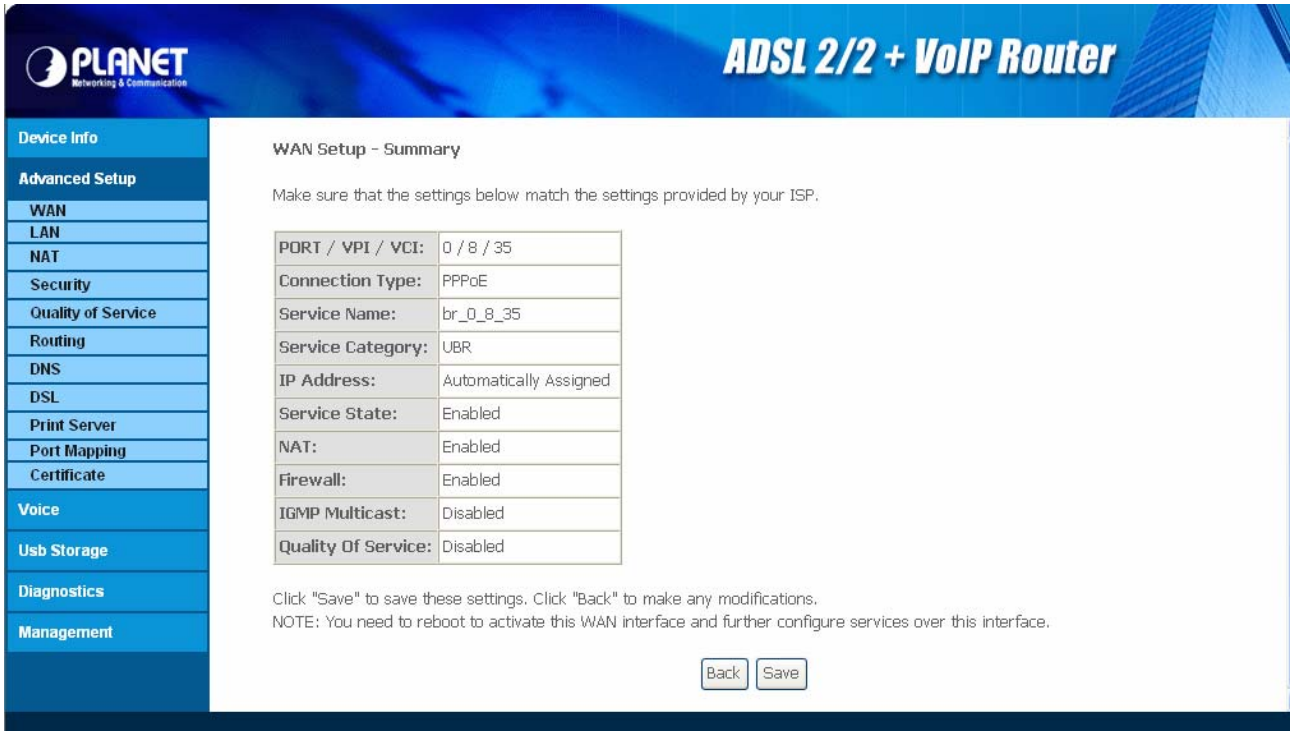


Figure: PPPoE Setup Summary

Click “Save” to save these settings.And you can click “Back” to make any modifications. After you click “Save”, it show the following interface.

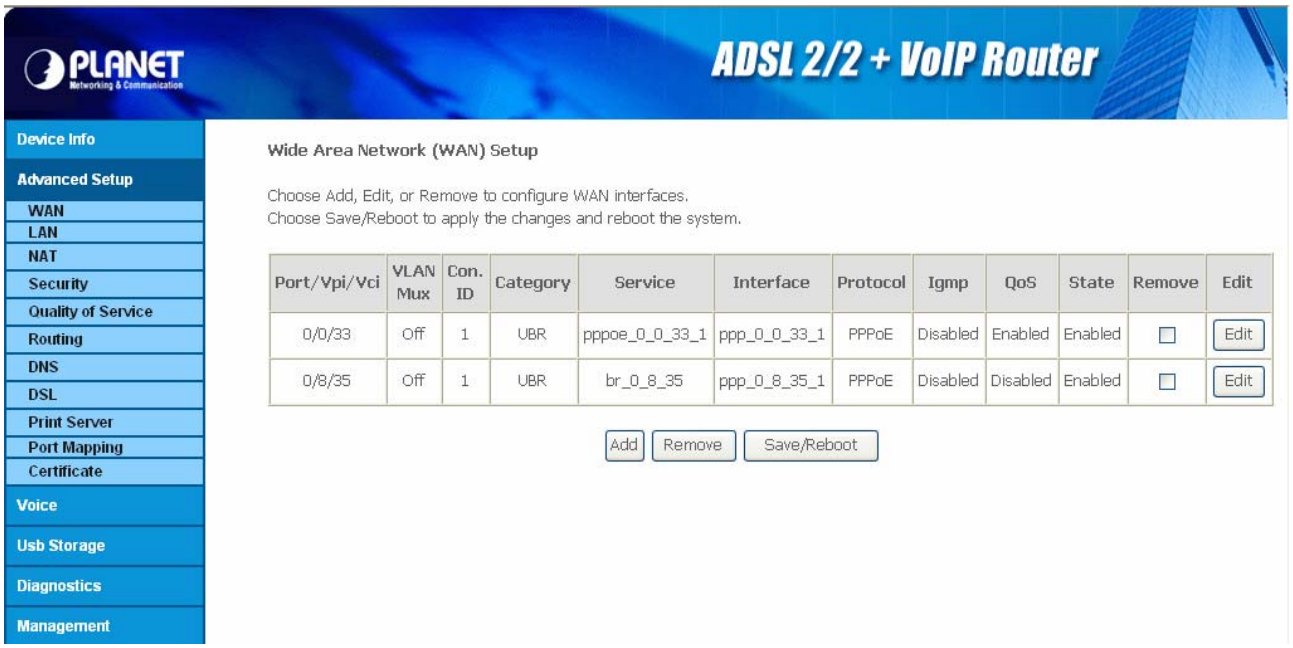


Figure: PPPoE Setup Complete

NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

3.3.1.2 Add PPPoA PVC

Click “Add” to add a certain piece of PVC. The following descriptions are given by an example of adding “PVC 8/35” (PPPOA mode).

1. Click “Add” following “PVC 8/35”.

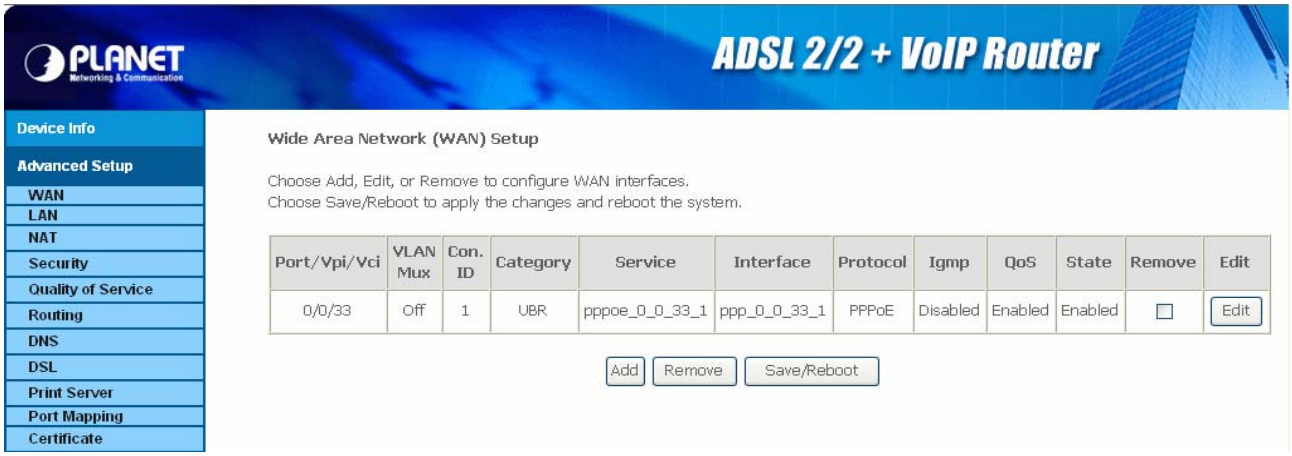


Figure: PPPoA Config

2. In this interface, you can modify VPI/VCIs, service categories and QoS.

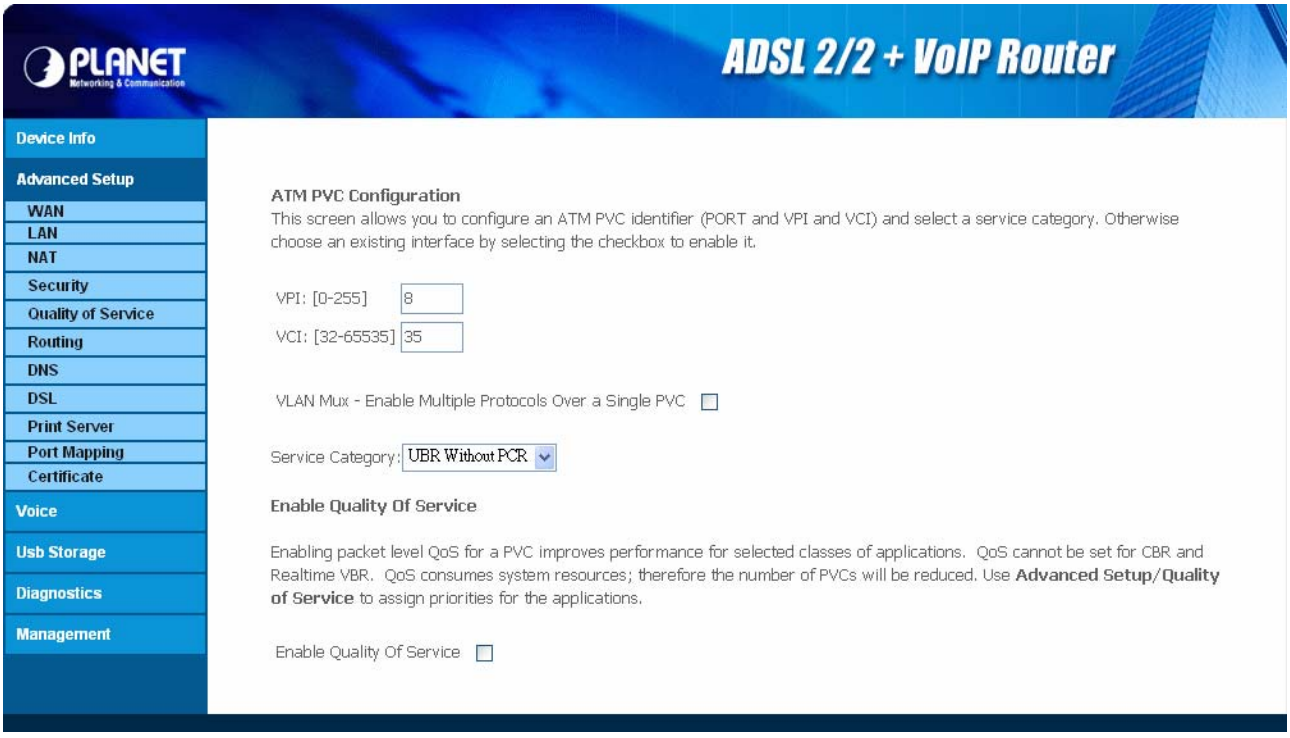

PLANET
ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
DNS
DSL
Print Server
Port Mapping
Certificate
Voice
Usb Storage
Diagnostics
Management
ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (PORT and VPI and VCI) and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.
VPI: [0-255] 8
VCI: [32-65535] 35
VLAN Mux - Enable Multiple Protocols Over a Single PVC
Service Category: UBR Without PCR
Enable Quality Of Service
Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Service to assign priorities for the applications.
Enable Quality Of Service

Figure: PVC and Qos config page

VPI (Virtual Path Identifier): The virtual path between two points in an ATM network, and its valid value is from 0 to 255.

VCI (Virtual Channel Identifier): The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols).

Service Category: UBR Without PCR/UBR With PCR/CBR/Non Realtime VBR/Realtime VBR.

Enable Quality Of Service: enable/disable.

In this example, PVC 8/35 is required to modify, so service category and QoS will remain default values. In actual applications, you can modify them depending on your practices.

After proper modifications, click “Next” to show the following interface.

3. In this interface, you can modify Internet Connection Type and Encapsulation Type.

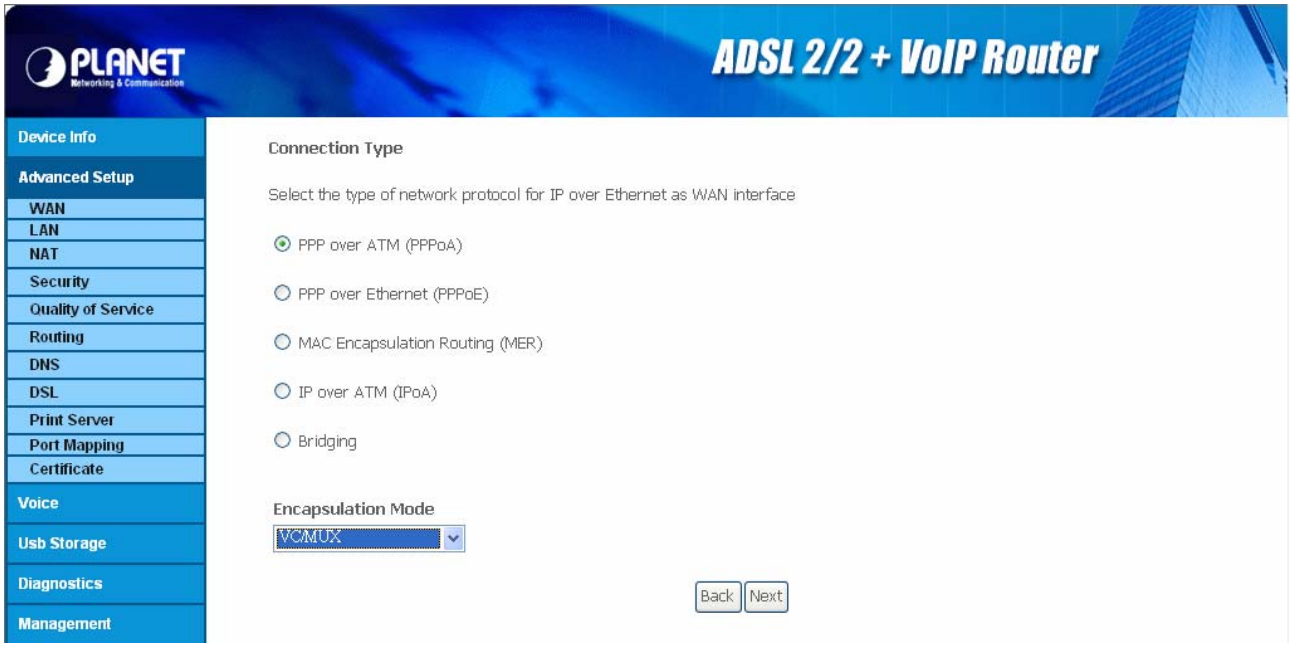


Figure: Internet Connection Type and Encapsulation Type page

Change the connection type of PVC 8/35 to “PPP over ATM (PPPoA)”.

Select “PPP over ATM (PPPoA)”, and “VC/MUX” (depending on the uplink equipment, generally “VC/MUX”) as “Encapsulation Mode”.

Click “Next” to show the following interface.

4. In this interface, you can modify the PPP Username, PPP Password, Authentication Method and so on.

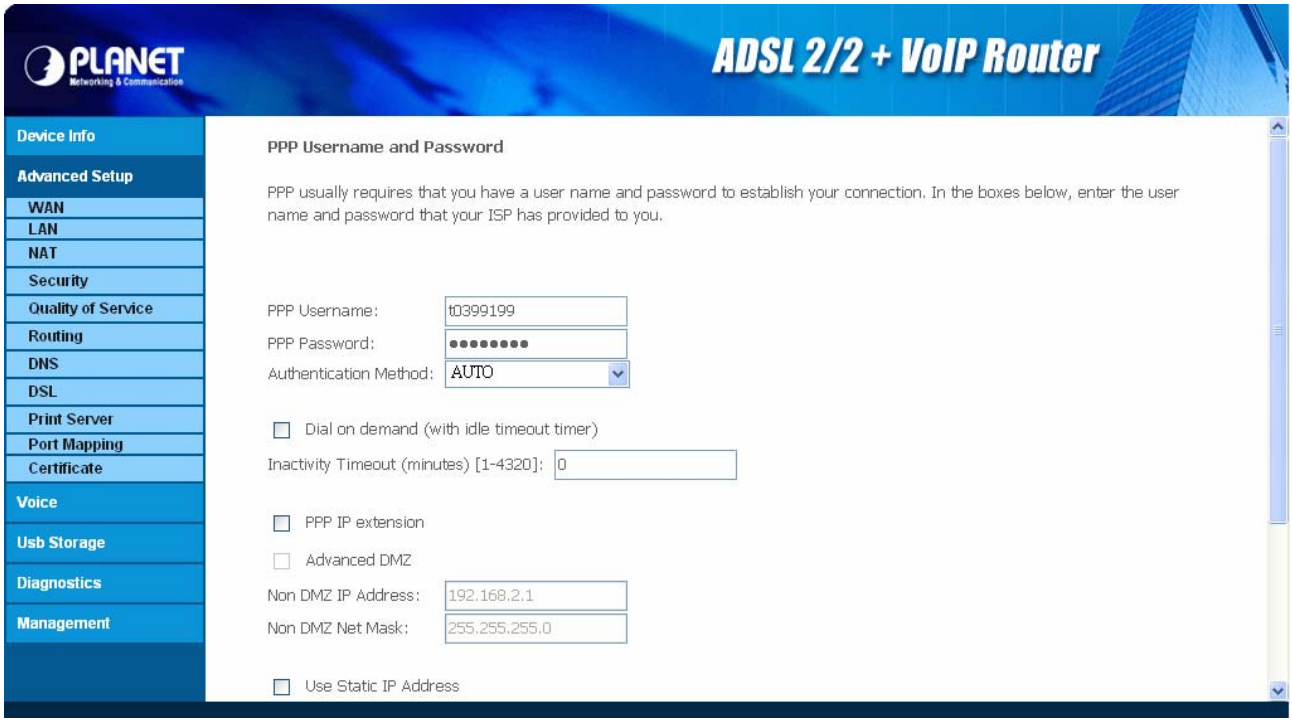


Figure: PPP information and others funtion page

PPP Username: the correct user name that your ISP has provided to you.

PPP Password: the correct password that your ISP has provided to you.

Authentication Method: AUTO, PAP, CHAP, MSCHAP. Usually select AUTO will be OK.

Dial on demand (with idle timeout timer): If enable it, you need to input the idle timeout time. Within the preset minutes, if the MODEM doesn't detect the flow of the user continuously, the MODEM will automatically disconnect the PPPOA connection. Once it detects the flow (like access to a webpage), the MODEM will restart the PPPOA dial up.

If disable it, the MODEM will perform PPPOA dial-up all the time. Unless the MODEM is powered off and DSLAM or uplink equipment are abnormal, the PPPOA connnection will not broken.

PPP IP extension: After "PPP IP extension" is enabled, the WAN IP address obtained by the MODEM through built-in dial-up can be directly assigned to the PC being attached with the MODEM (at this time, the MODEM has only one PC). From the view of the PC user, this is even with that the PC dials up to obtain an IP addres. But actually, the dial-up is done by the MODEM.

If disable it, the MODEM obtain the WAN IP address itself.

Advanced DMZ: This is the virtual server configuration option. The DMZ Host feature allows one local computer to be exposed to the internet, to be this feature,the other computer can easily enter the DMZ Host, a DMZ host is not protected by the firewall and may be vulnerable to attack. Designating a DMZ host may also put other computers in the home network at risk. When designating a DMZ host, you must consider the security implications and protect it if necessary.

a. If you want to setup DMZ Host, you should enable the “PPP IP extension” at first;
b. **Non DMZ IP Address:** The DMZ Host IP Address, you can modify it by hand;
c. **Non DMZ Net Mask:** The DMZ Host Subnet Mask, it is build upon the DMZ Host IP Address.

Use Static IP Address: If disabled it, the MODEM through PPPOA dial-up, to obtain an IP address assigned by an uplink equipment such as BAS.

If enable it, the MODEM use this IP as the WAN IP address.

After input the PPP Username and PPP Password, click “Next” to show the following interface.

5. In this interface, you can modify the Service name and enable/disable the IGMP Multicast, WAN Service.

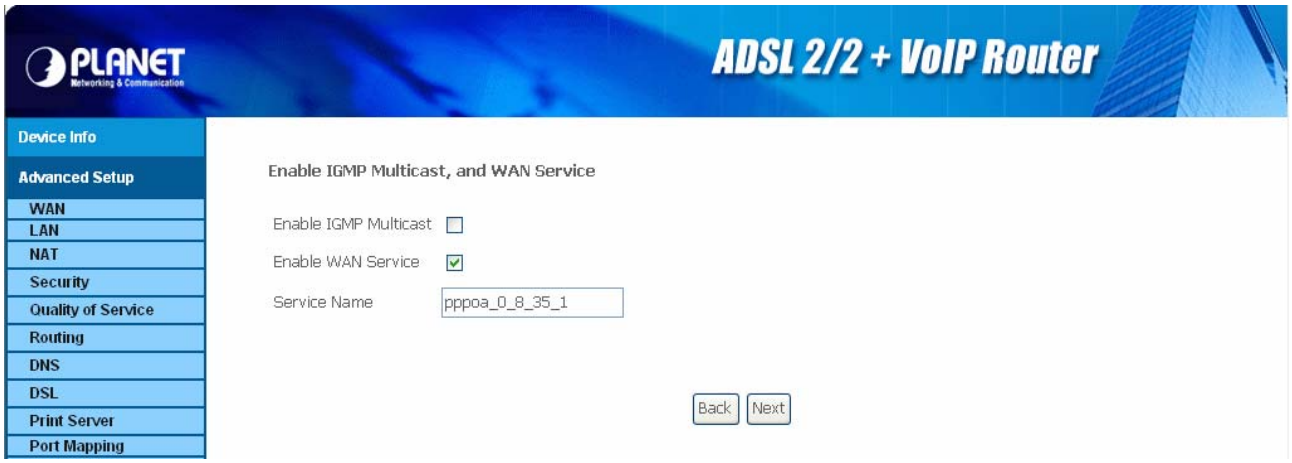


Figure: PPPoA IGMP and WAN service page

IGMP Multicast: IGMP proxy. For example, if you need PPPoA mode support IPTV, please enable it.

WAN Service: Please enable it, unless you don’t need to active the PVC.

Click “Next” to show the following interface.

6. In this interface, it show the all configuration. You can see some default values: NAT enable, Firewall enable.

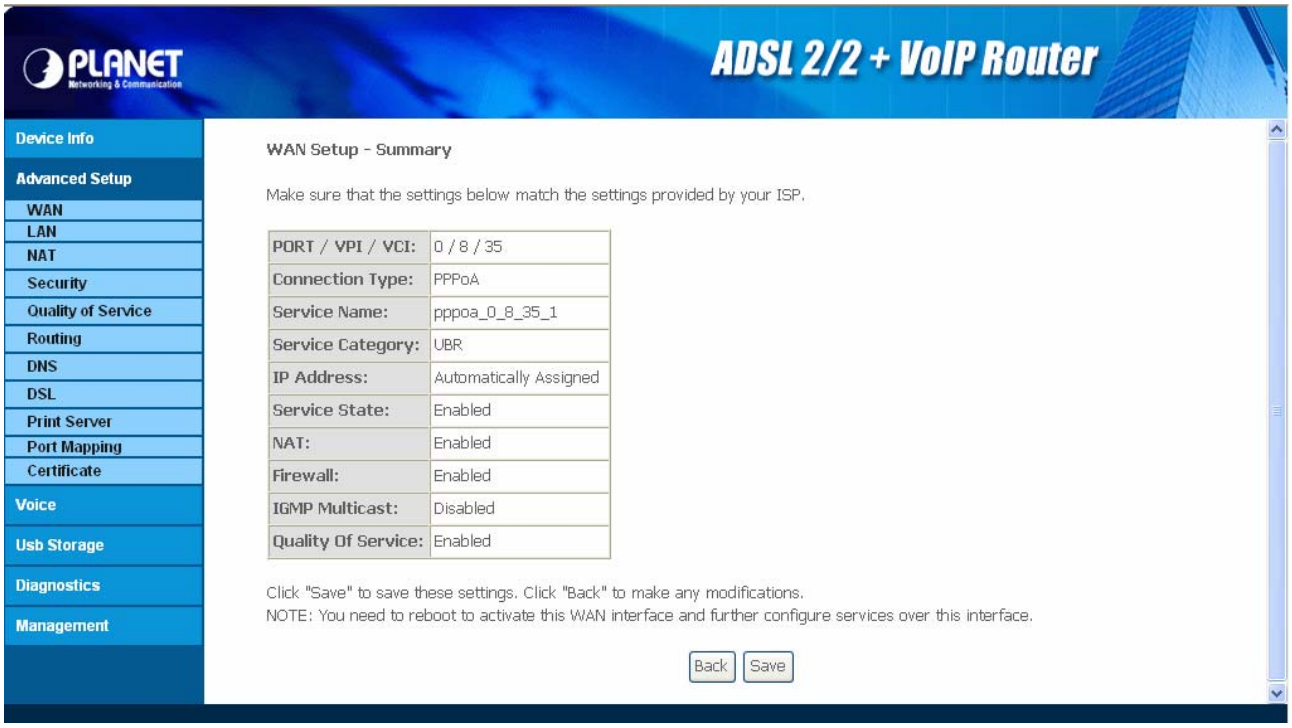


Figure: PPPoA Setup Summary

Click “Save” to save these settings.And you can click “Back” to make any modifications. After you click “Save”, it show the following interface.

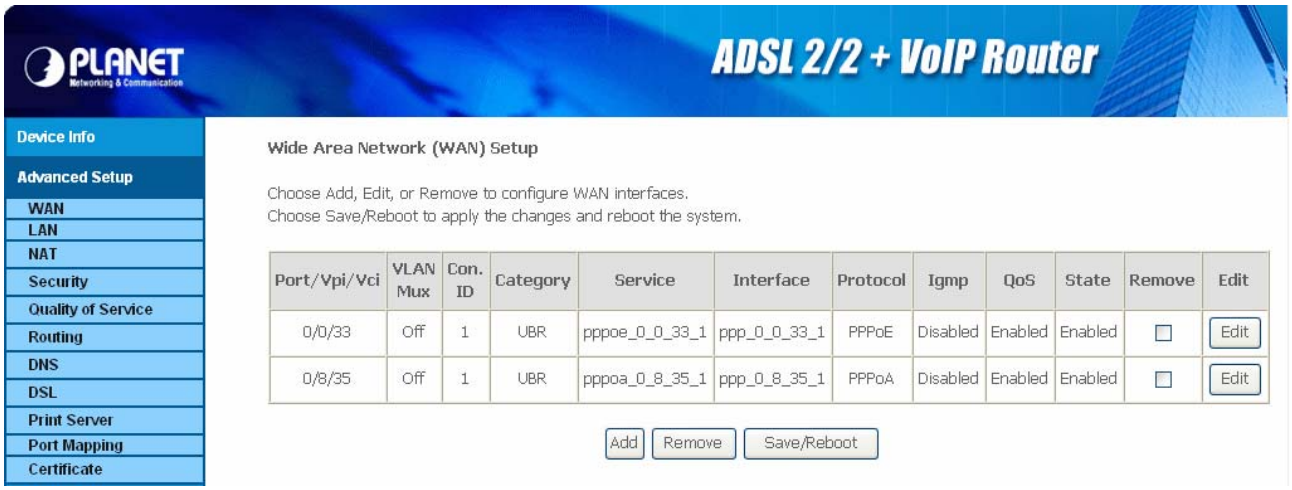


Figure: PPPoA Setup Complete

NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

3.3.1.3 Add MER PVC

Click “Add” to add a certain piece of PVC. The following descriptions are given by an example of adding “PVC 8/35” (MER mode).

1. Click “Add” following “PVC 8/35”.

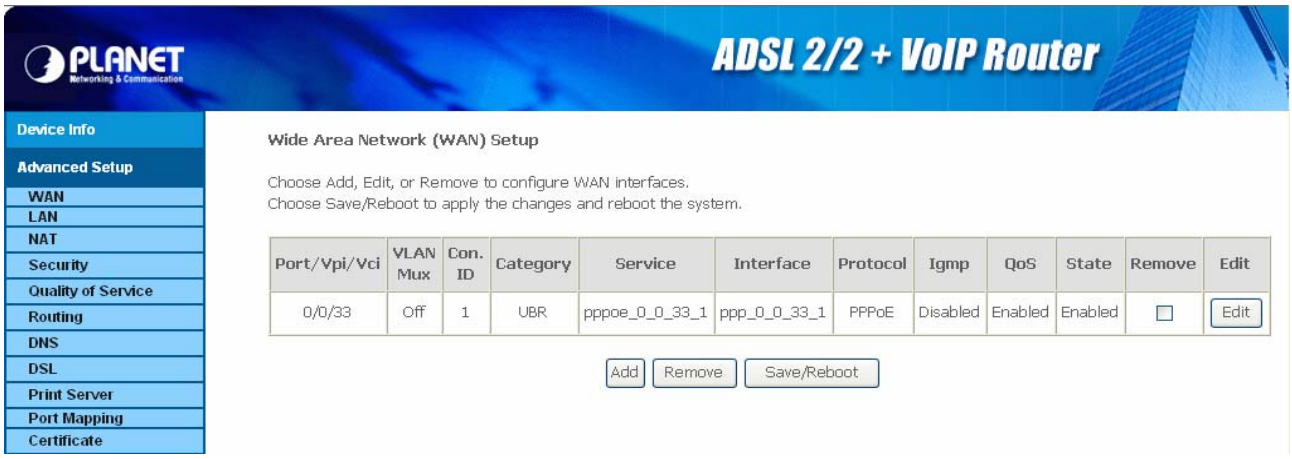


Figure: MER Config

2. In this interface, you can modify VPI/VCIs, service categories and QoS.

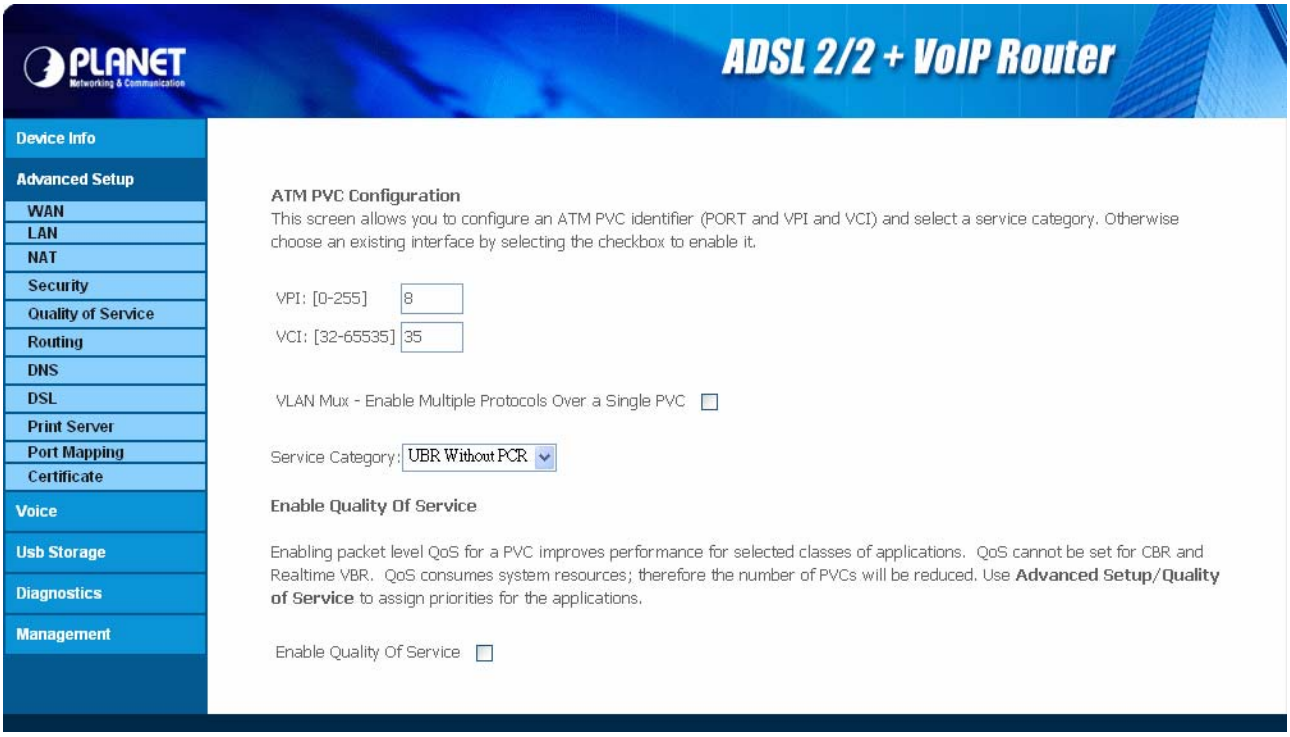

ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
DNS
DSL
Print Server
Port Mapping
Certificate
Voice
Usb Storage
Diagnostics
Management
ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (PORT and VPI and VCI) and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.
VPI: [0-255] 8
VCI: [32-65535] 35
VLAN Mux - Enable Multiple Protocols Over a Single PVC
Service Category: UBR Without PCR
Enable Quality Of Service
Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Service to assign priorities for the applications.
Enable Quality Of Service

Figure: PVC and it’s Qos config page

VPI (Virtual Path Identifier): The virtual path between two points in an ATM network, and its valid value is from 0 to 255.

VCI (Virtual Channel Identifier): The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols).

Service Category: UBR Without PCR/UBR With PCR/CBR/Non Realtime VBR/Realtime VBR.

Enable Quality Of Service: enable/disable.

In this example, PVC 8/35 is required to modify, so service category and QoS will remain default values. In actual applications, you can modify them depending on your practices.

After proper modifications, click “Next” to show the following interface.

3. In this interface, you can modify Internet Connection Type and Encapsulation Type.

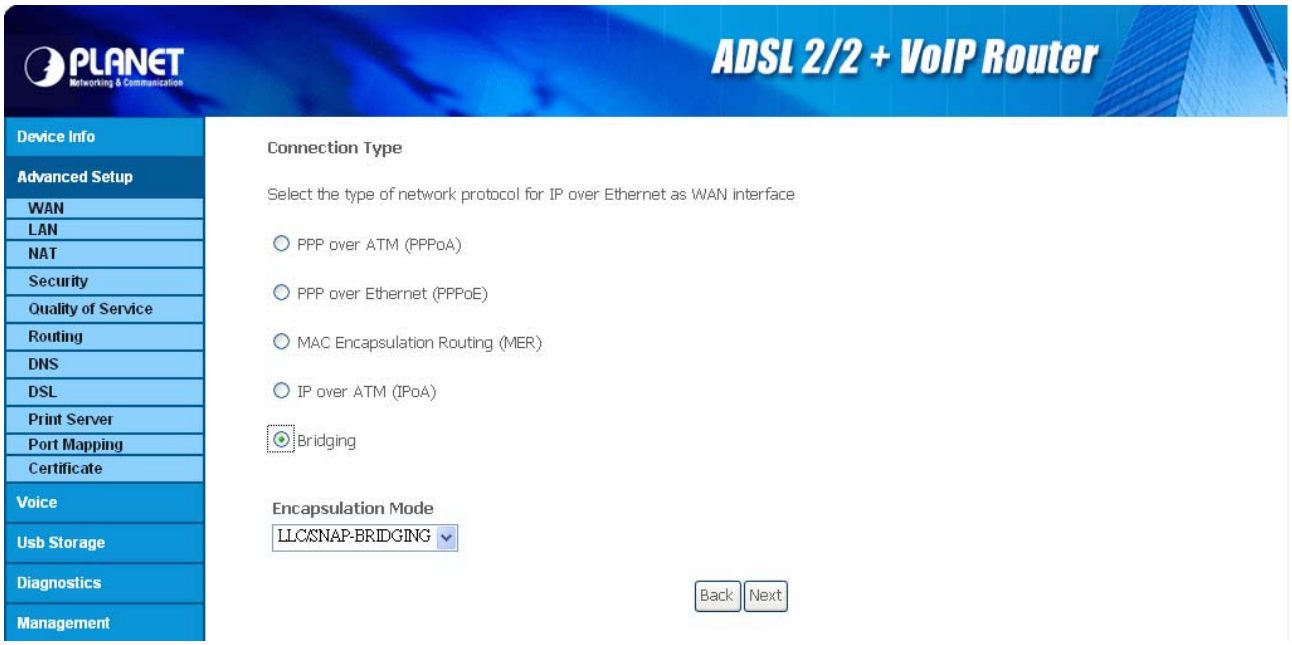


Figure: Internet Connection Type and Encapsulation Type page

Change the connection type of PVC 8/35 to “MAC Encapsulation Routing (MER)”.

Select “MAC Encapsulation Routing (MER)”, and “LLC/SNAP-BRIDGING” (depending on the uplink equipment, generally “LLC/SNAP-BRIDGING”) as “Encapsulation Mode”.

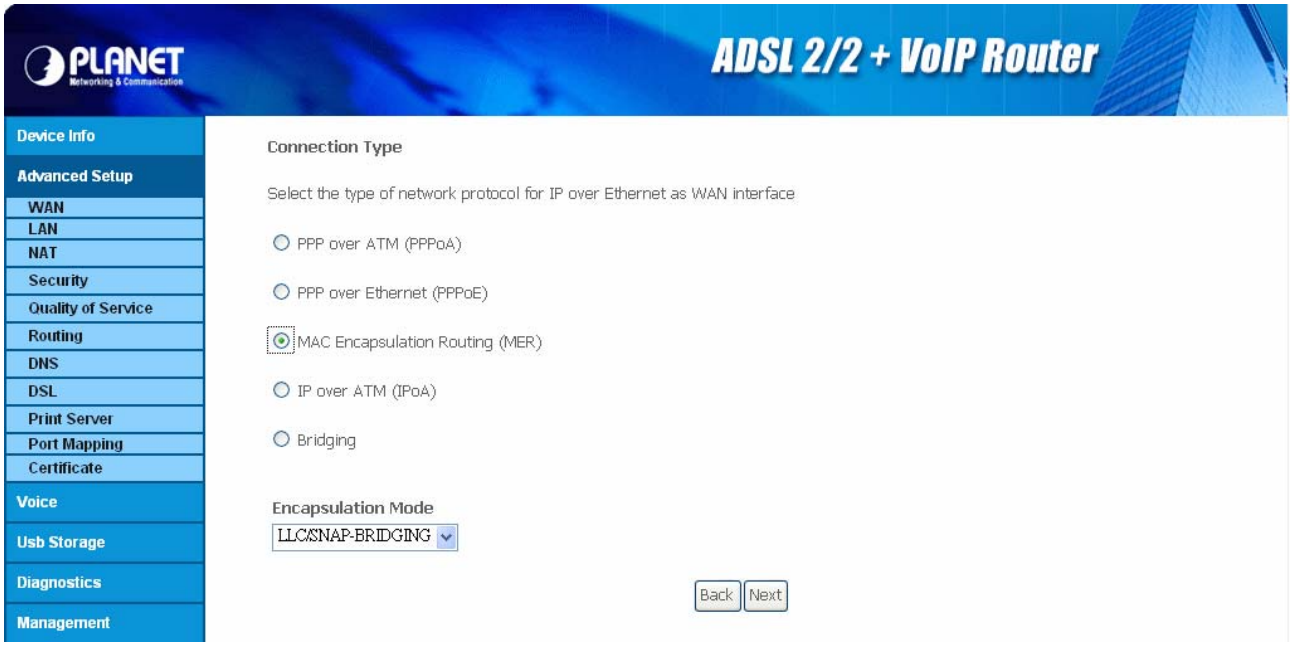


Figure: MAC Encapsulation Routing (MER)

Enable 802.1q: If enable it, input the 802.1q VLAN tag value. Note that 802.1q VLAN tagging is only available for PPPoE, MER and Bridge.

Click “Next” to show the following interface.

4. In this interface, you can modify the WAN IP address, Default Gateway and DNS Server settings.

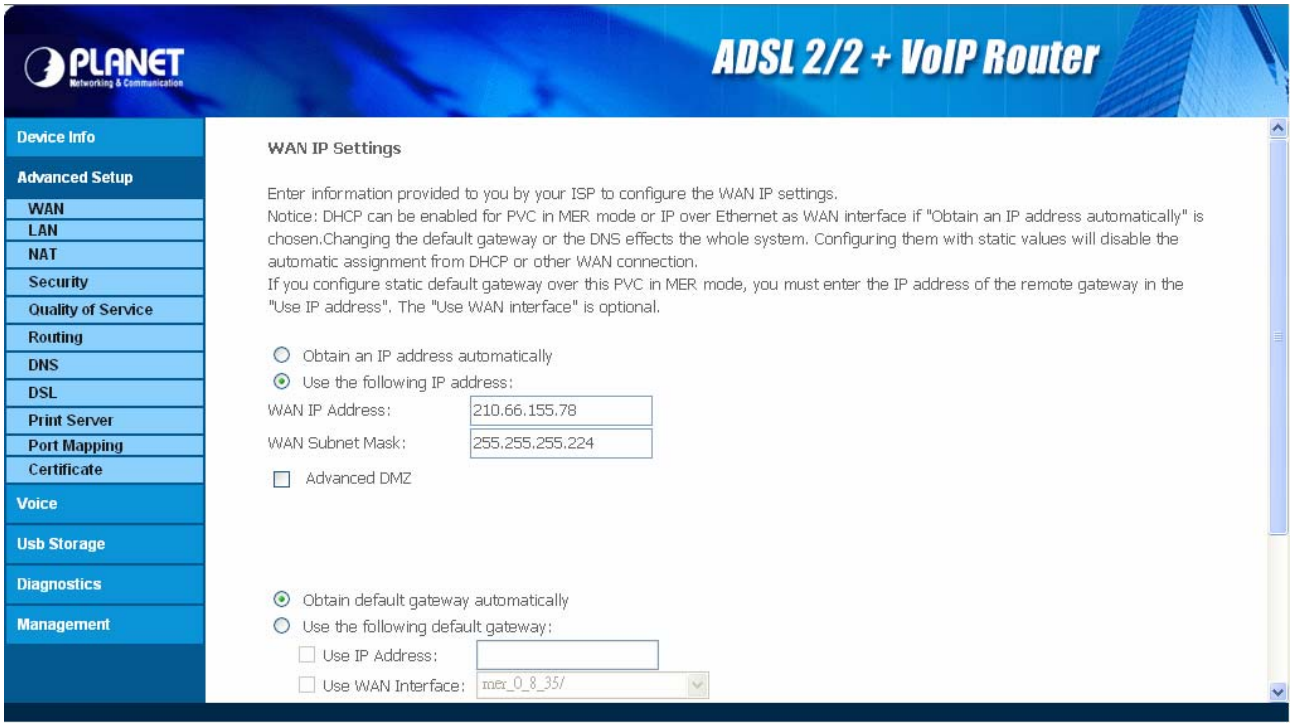

PLANET
ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
DNS
DSL
Print Server
Port Mapping
Certificate
Voice
Usb Storage
Diagnostics
Management
WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: DHCP can be enabled for PVC in MER mode or IP over Ethernet as WAN interface if "Obtain an IP address automatically" is chosen.Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.
If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address". The "Use WAN interface" is optional.
Obtain an IP address automatically
Use the following IP address:
WAN IP Address: 210.66.155.78
WAN Subnet Mask: 255.255.255.224
Advanced DMZ
Obtain default gateway automatically
Use the following default gateway:
Use IP Address:
Use WAN Interface: mer_0_8_35/

Figure: MER WAN IP config page

Obtain an IP address automatically: The MODEM will obtain a (WAN) IP address automatically and at this time it will enable DHCP Client functions. The WAN IP address is obtained from the uplink equipment like BAS and the uplink equipment is required to enable the DHCP Server functions.

Use the following IP address: If you want to input the WAN IP address by yourself. Check this entry and then input related data in the field.

WAN IP Address: Input the IP address of the WAN interface provided by your ISP.

WAN Subnet Mask: Input the subnet mask concerned to the IP address of the WAN interface provided by your ISP.

Obtain Default Gateway automatically: To obtain the IP address of the default gateway assigned by the uplink equipment such as BRAS.

Use the following Default Gateway: If you want to input the IP address of the default gateway by yourself, click this entry and then input related data in the fields.

Use IP Address: Input the gateway of the WAN interface provided by your ISP.

Use WAN Interface: As to BAS equipment, it is the IP address of the downlink interface.

Obtain DNS server address automatically: To obtain the IP address of the DNS server assigned by the uplink equipment such as BRAS.

Use the following DNS server addesses: If you want to input the IP address of the DNS server by yourself, click this entry and then input related data in the fields.

Primary DNS server: Input the IP address of the primary DNS server here.

Secondary DNS server: Input the IP address of the secondary DNS server provided by your ISP here.

After correctly modifications, click “Next” to show the following interface.

5. In this interface, you can modify the Service name and enable/disable the NAT, Firewal, IGMP Multicast, WAN Service.

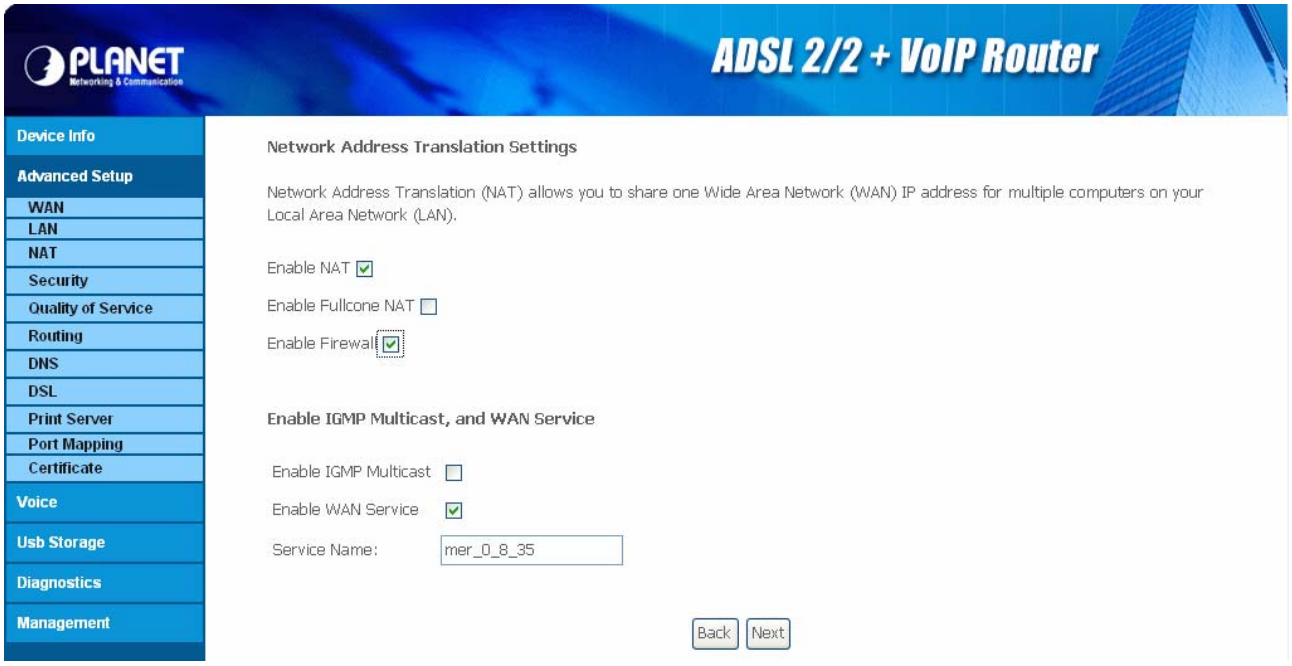


Figure: MER IGMP and WAN service page

Enable NAT: Select it to enable the NAT functions of the MODEM. If you are not to enable NAT and intend the user of the MODEM to access the Internet normally, you must add a route on the uplink equipment; otherwise the access to the Internet will fail. Normally, it is required to enable NAT.

Enable Firewall: enable/disable IP filtering.

IGMP Multicast: IGMP proxy. For example, if you need MER mode support IPTV, please enable it.

WAN Service: Please enable it, unless you don’t need to active the PVC.

Click “Next” to show the following interface.

6. In this interface, it show the all configuration.

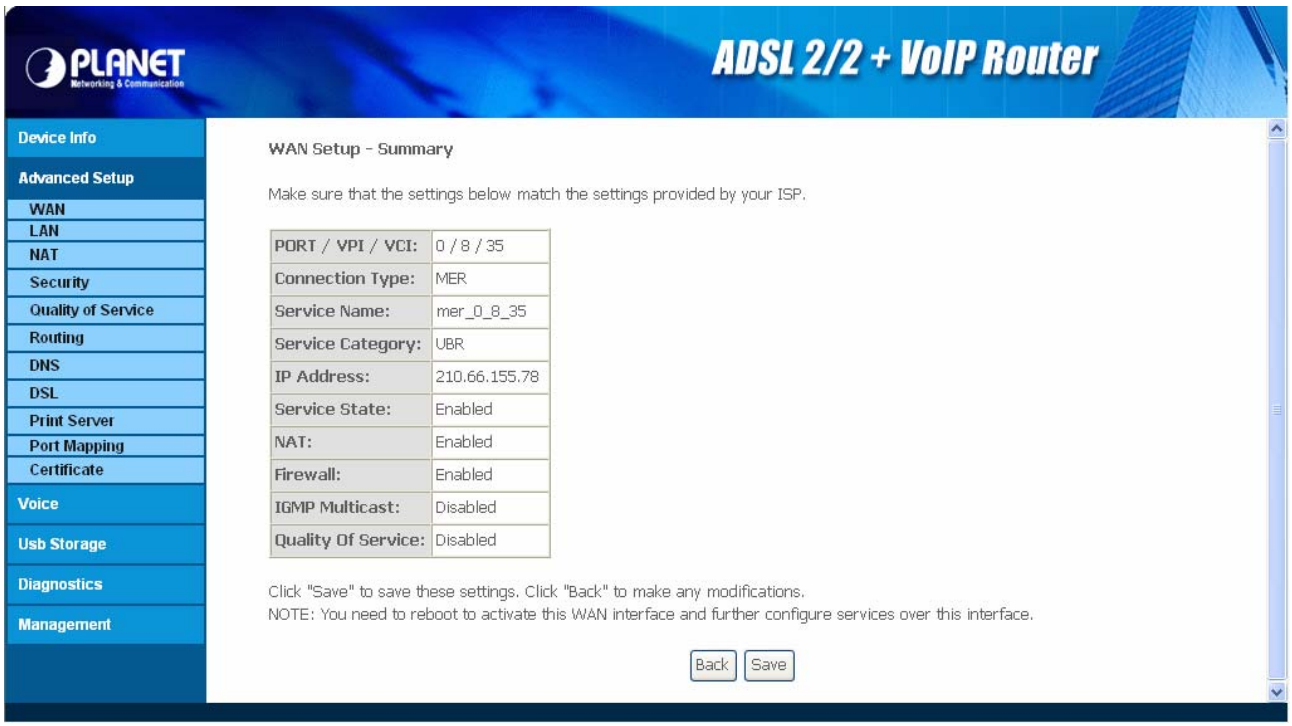


Figure: MER Setup Summary

Click “Save” to save these settings.And you can click “Back” to make any modifications. After you click “Save”, it show the following interface.

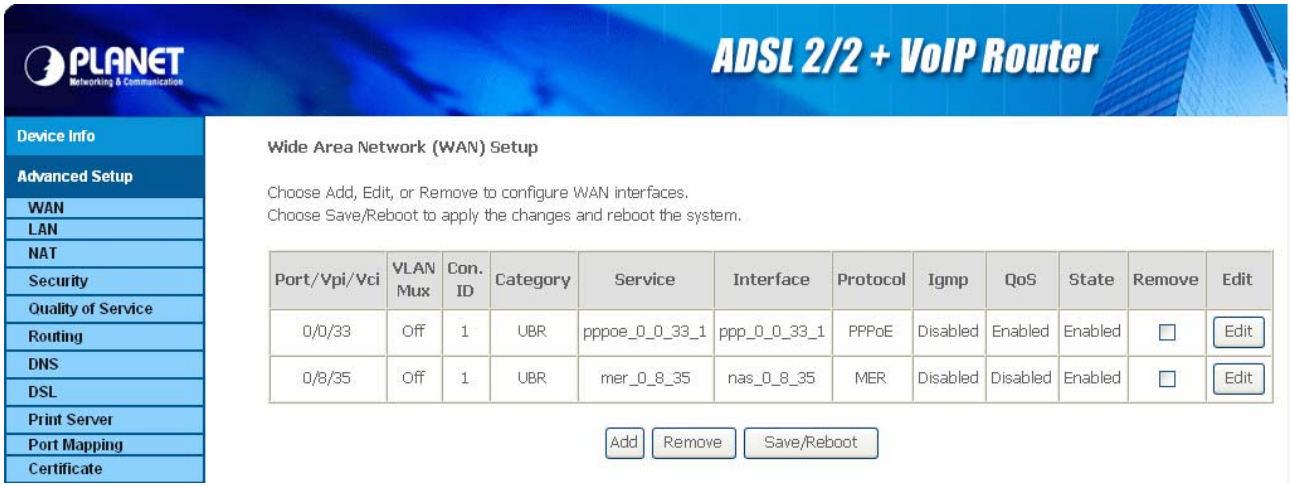


Figure: MER Setup Complete

NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

3.3.1.4 Add IPoA PVC

Click “Add” to add a certain piece of PVC. The following descriptions are given by an example of adding “PVC 8/35” (IPoA mode).

1. Click “Add” following “PVC 8/35”.

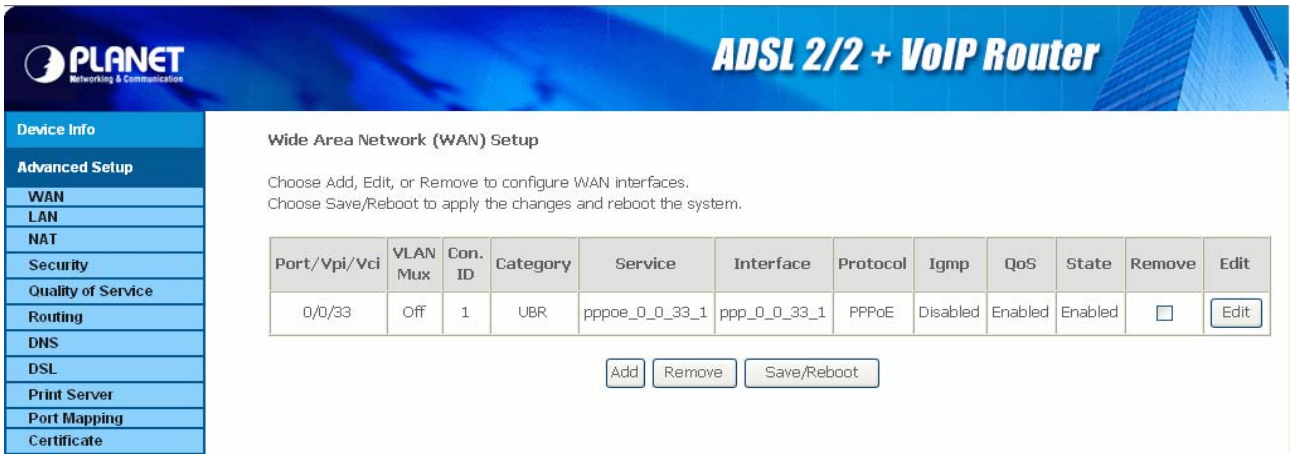


Figure: IPoA Config

2. In this interface, you can modify VPI/VCIs, service categories and QoS.

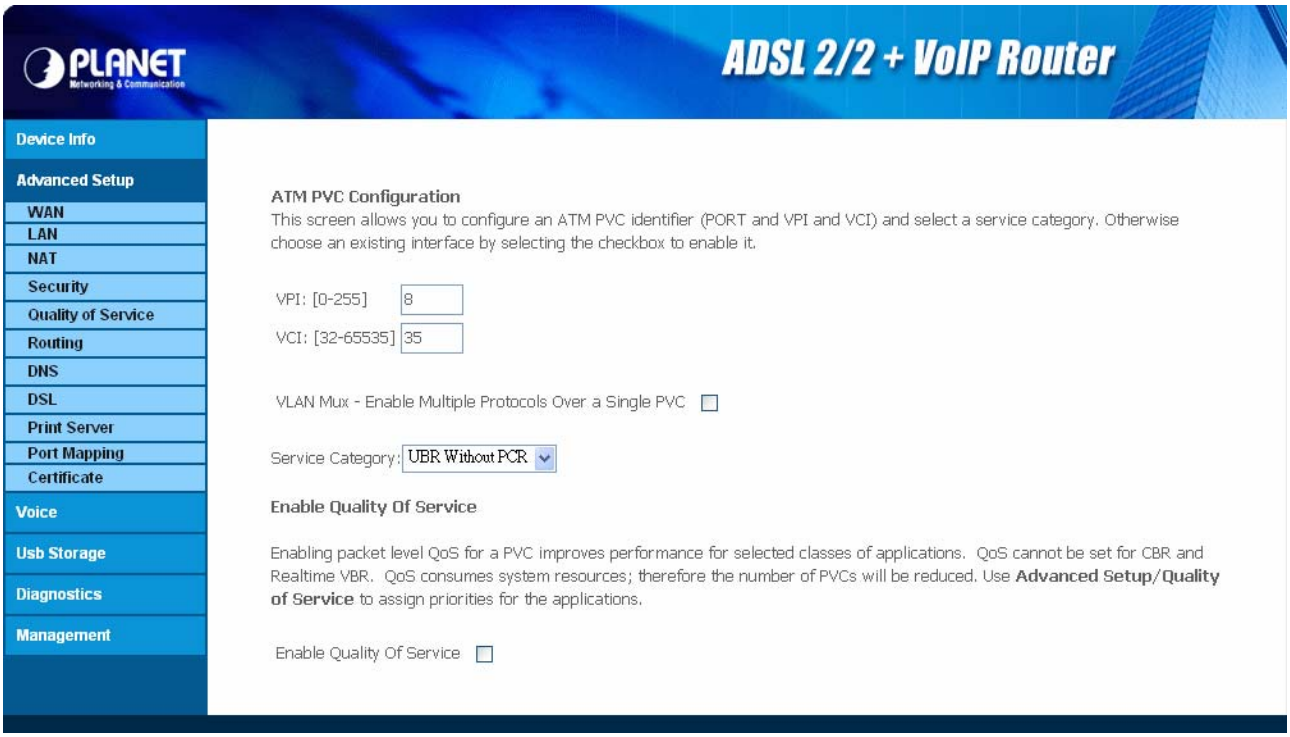

PLANET
ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
DNS
DSL
Print Server
Port Mapping
Certificate
Voice
Usb Storage
Diagnostics
Management
ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (PORT and VPI and VCI) and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.
VPI: [0-255] 8
VCI: [32-65535] 35
VLAN Mux - Enable Multiple Protocols Over a Single PVC
Service Category: UBR Without PCR
Enable Quality Of Service
Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Service to assign priorities for the applications.
Enable Quality Of Service

Figure: PVC and Qos config page

VPI (Virtual Path Identifier): The virtual path between two points in an ATM network, and its valid value is from 0 to 255.

VCI (Virtual Channel Identifier): The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols).

Service Category: UBR Without PCR/UBR With PCR/CBR/Non Realtime VBR/Realtime VBR.

Enable Quality Of Service: enable/disable.

In this example, PVC 8/35 is required to modify, so service category and QoS will remain default values. In actual applications, you can modify them depending on your practices.

After proper modifications, click “Next” to show the following interface.

3. In this interface, you can modify Internet Connection Type and Encapsulation Type.

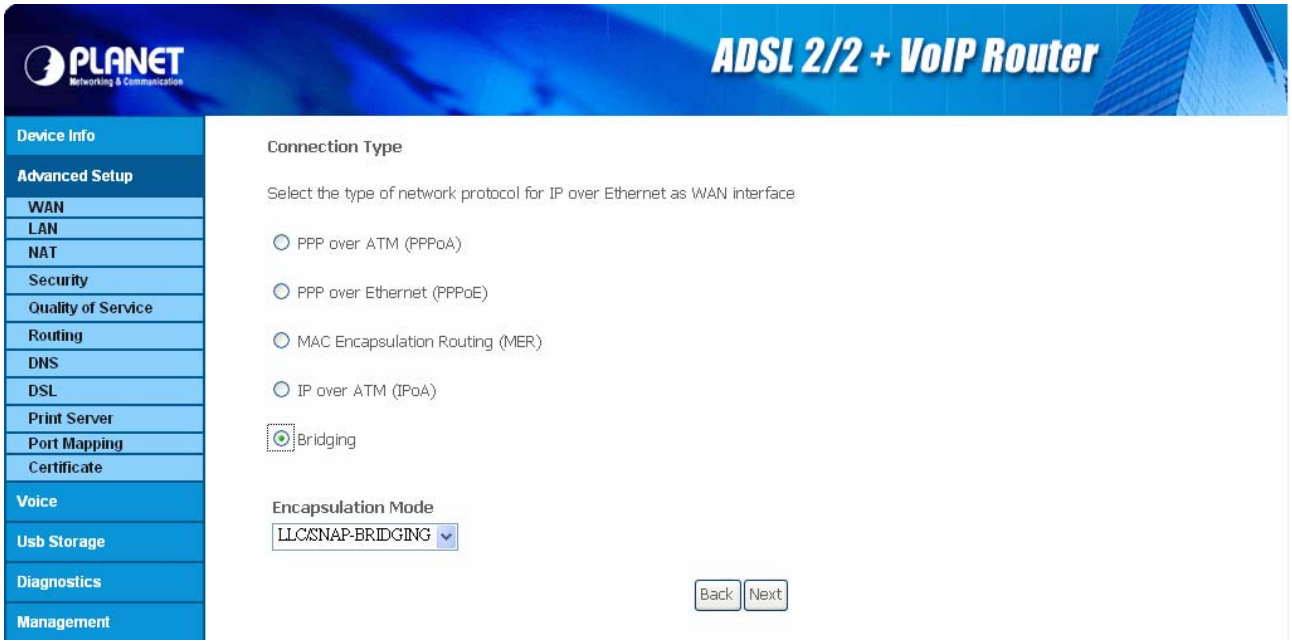


Figure: Internet Connection Type and Encapsulation Type page

Change the connection type of PVC 8/35 to “IP over ATM (IPoA)”.

Select “IP over ATM (IPoA)”, and “LLC/SNAP-ROUTING” (depending on the uplink equipment, generally “LLC/SNAP-ROUTING”) as “Encapsulation Mode”.

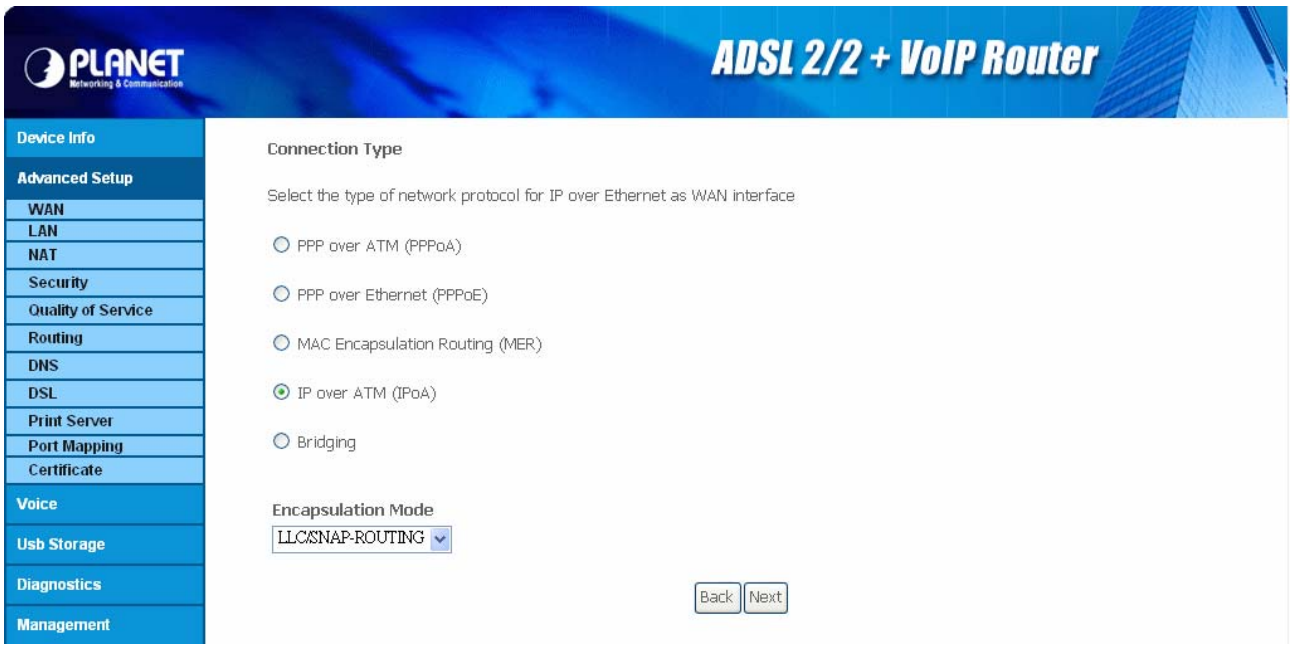


Figure: IP over ATM (IPoA)

Click “Next” to show the following interface.

4. In this interface, you can modify the WAN IP, Default Gateway and DNS Server settings.

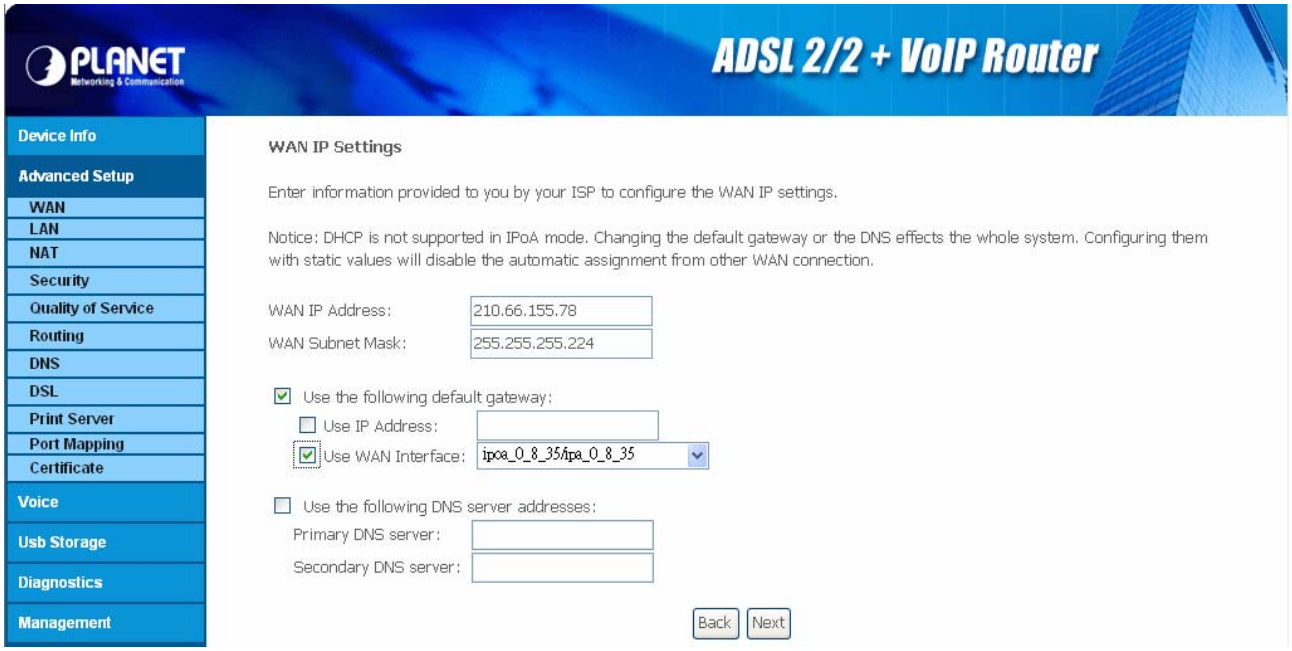


Figure: IPoA WAN IP Setting

WAN IP Address: Input the IP address of the WAN interface provided by your ISP.

WAN Subnet Mask: Input the subnet mask concerned to the IP address of the WAN interface provided by your ISP.

Obtain Default Gateway automatically: To obtain the IP address of the default gateway assigned by the uplink equipment such as BRAS.

Use the following Default Gateway: If you want to input the IP address of the default gateway by yourself, click this entry and then input related data in the fields.

Otherwise to obtain the IP address of the default gateway assigned by the uplink equipment such as BRAS.

Use IP Address: Input the gateway of the WAN interface provided by your ISP.

Use WAN Interface: As to BAS equipment, it is the IP address of the downlink interface.

Obtain DNS server address automatically: To obtain the IP address of the DNS server assigned by the uplink equipment such as BRAS.

Use the following DNS server addesses: If you want to input the IP address of the DNS server by yourself, click this entry and then input related data in the fields.

Primary DNS server: Input the IP address of the primary DNS server here.

Secondary DNS server: Input the IP address of the secondary DNS server provided by your ISP here.

After correctly modifications, click “Next” to show the following interface.

5. In this interface, you can modify the Service name and enable/disable the NAT, Firewal, IGMP Multicast, WAN Service.

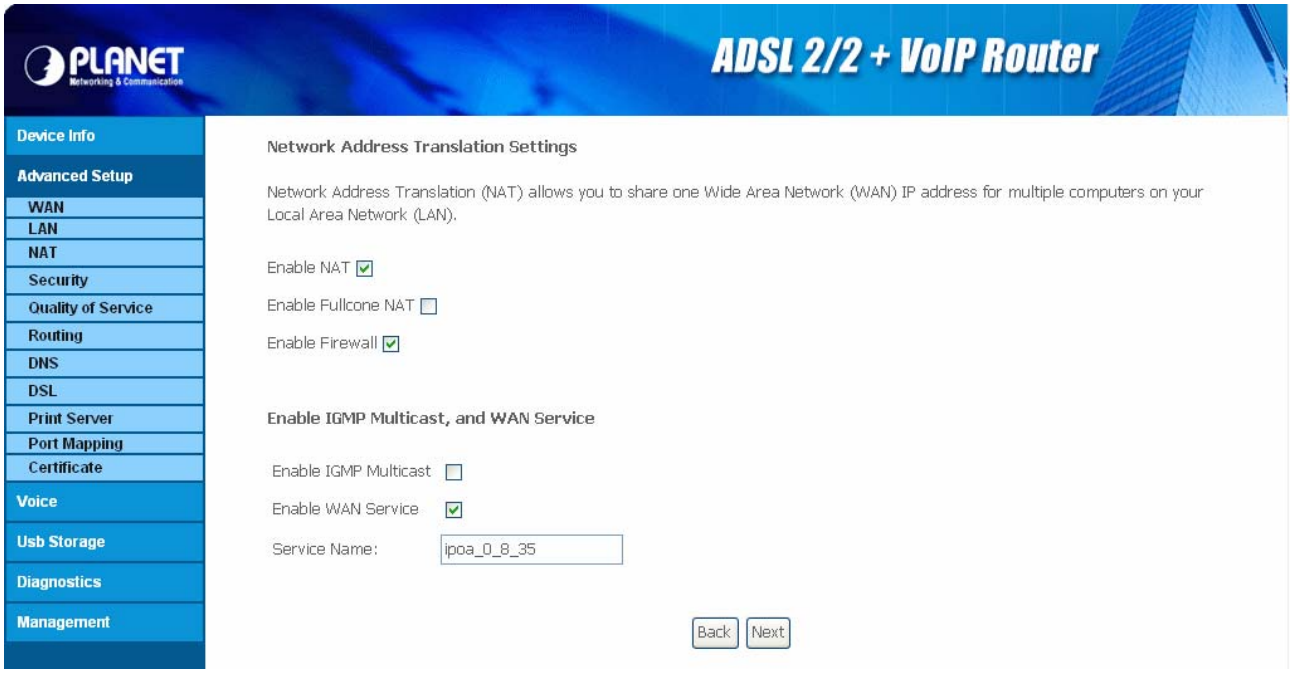


Figure: IPoA IGMP and WAN service page

Enable NAT: Select it to enable the NAT functions of the MODEM. If you are not to enable NAT and intend the user of the MODEM to access the Internet normally, you must add a route on the uplink equipment; otherwise the access to the Internet will fail. Normally, it is required to enable NAT.

Enable Firewall: enable/disable IP filtering.

IGMP Multicast: IGMP proxy. For example, if you need IPoA mode support IPTV, please enable it.

WAN Service: Please enable it, unless you don’t need to active the PVC.

Click “Next” to show the following interface.

6. In this interface, it show the all configuration.

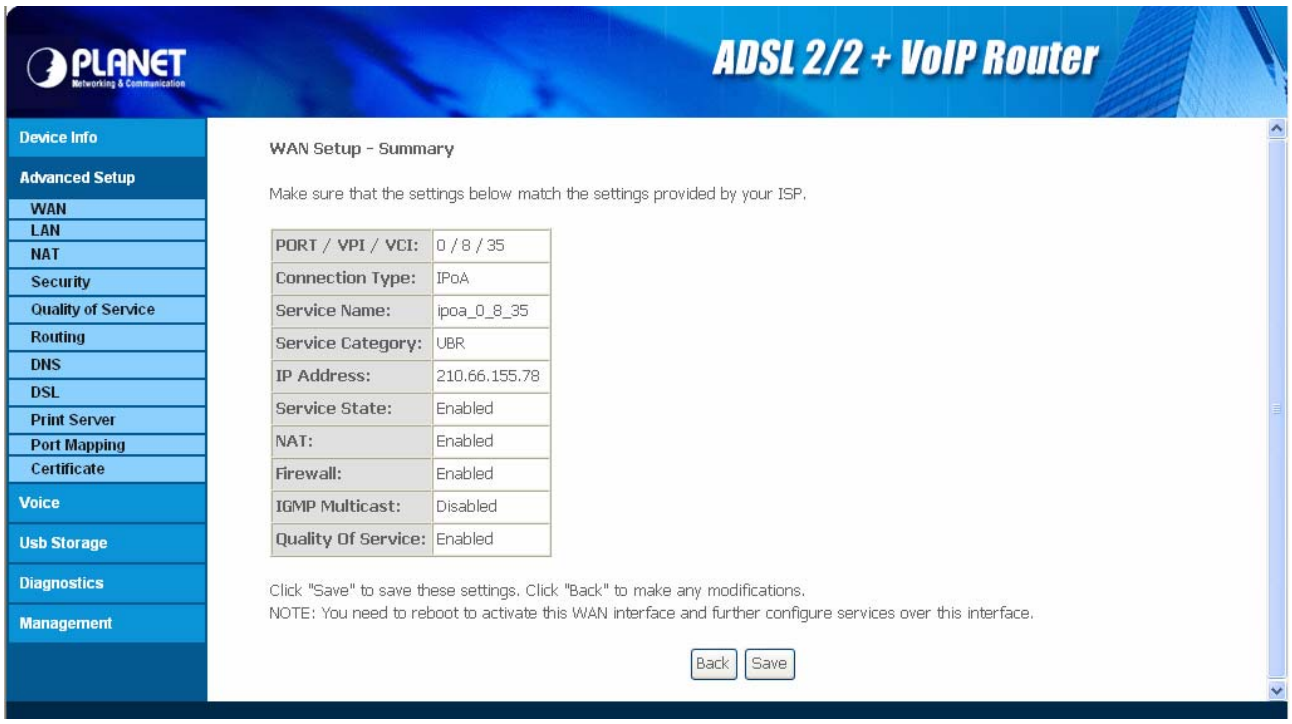


Figure: IPoA Setup Summary

Click “Save” to save these settings.And you can click “Back” to make any modifications. After you click “Save”, it show the following interface.

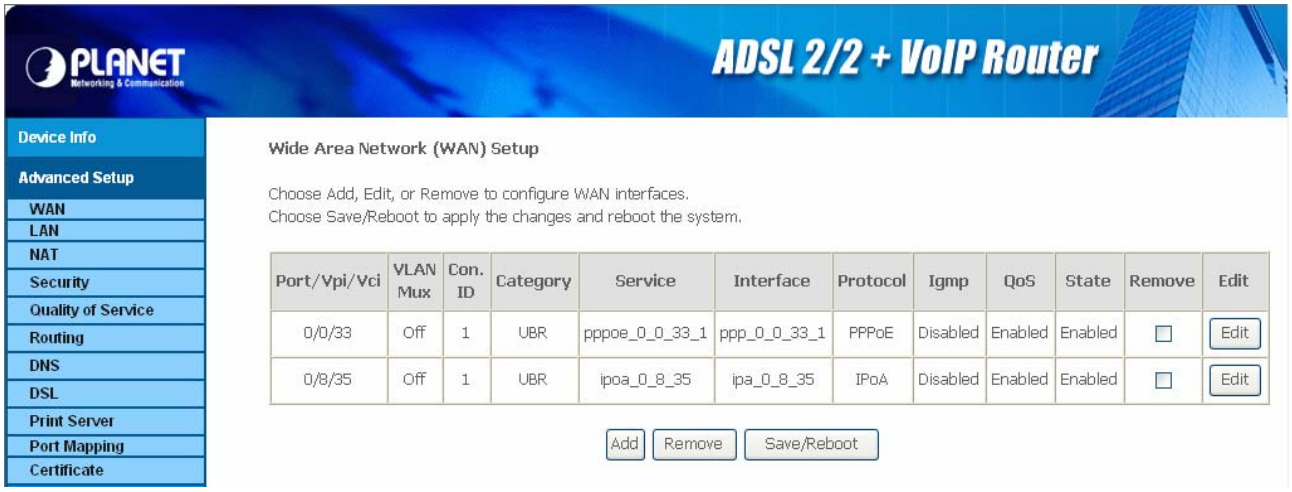


Figure: IPoA Setup Complete

NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

3.3.1.5 Add Bridge PVC

Click “Add” to add a certain piece of PVC. The following descriptions are given by an example of adding “PVC 8/35” (Bridge mode).

1. Click “Add” following “PVC 8/35”.

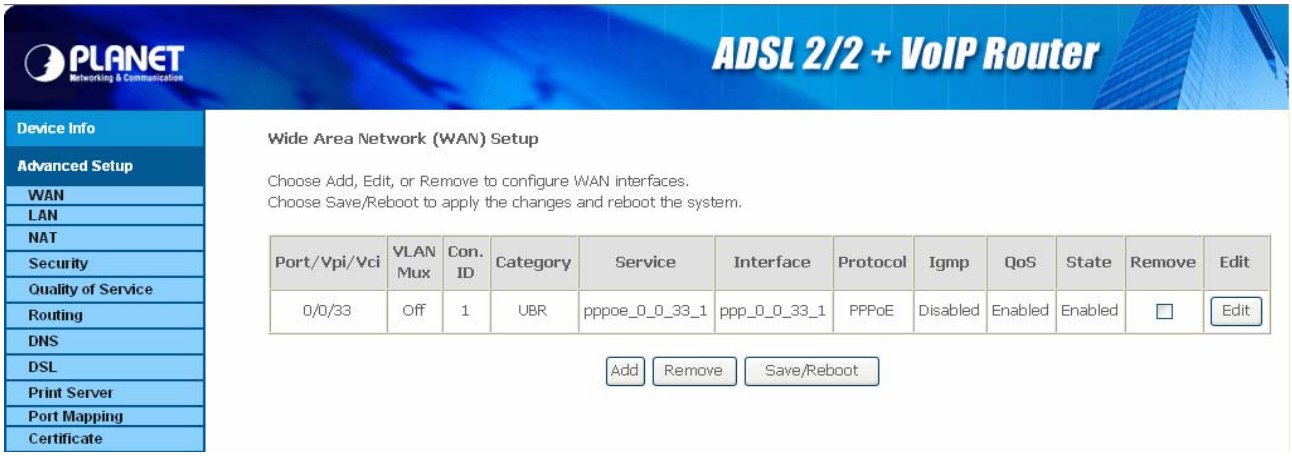


Figure: Bridge Config

2. In this interface, you can modify VPI/VCIs, service categories and QoS.

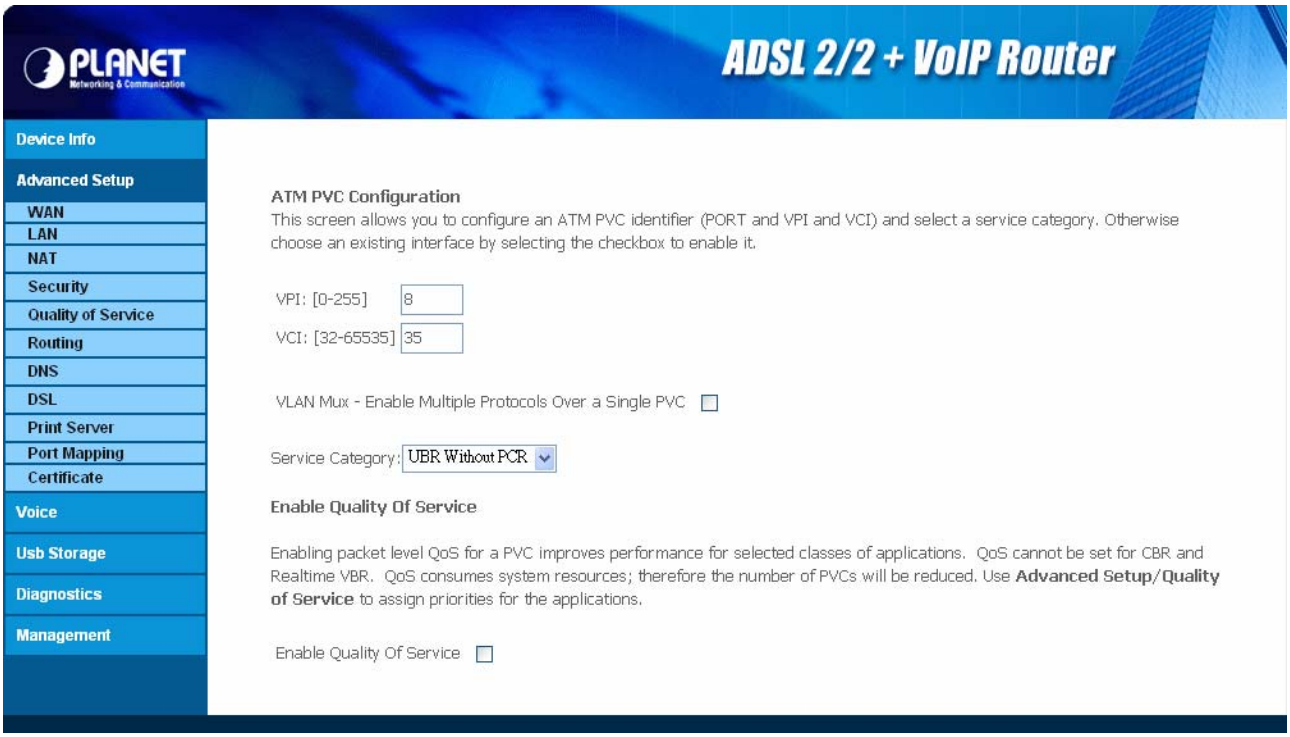

PLANET
ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
DNS
DSL
Print Server
Port Mapping
Certificate
Voice
Usb Storage
Diagnostics
Management
ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (PORT and VPI and VCI) and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.
VPI: [0-255] 8
VCI: [32-65535] 35
VLAN Mux - Enable Multiple Protocols Over a Single PVC
Service Category: UBR Without PCR
Enable Quality Of Service
Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Service to assign priorities for the applications.
Enable Quality Of Service

Figure: Internet Connection Type and Encapsulation Type page

VPI (Virtual Path Identifier): The virtual path between two points in an ATM network, and its valid value is from 0 to 255.

VCI (Virtual Channel Identifier): The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols).

Service Category: UBR Without PCR/UBR With PCR/CBR/Non Realtime VBR/Realtime VBR.

Enable Quality Of Service: enable/disable.

In this example, PVC 8/35 is required to modify, so service category and QoS will remain default values. In actual applications, you can modify them depending on your practices.

After proper modifications, click “Next” to show the following interface.

3. In this interface, you can modify Internet Connection Type and Encapsulation Type.

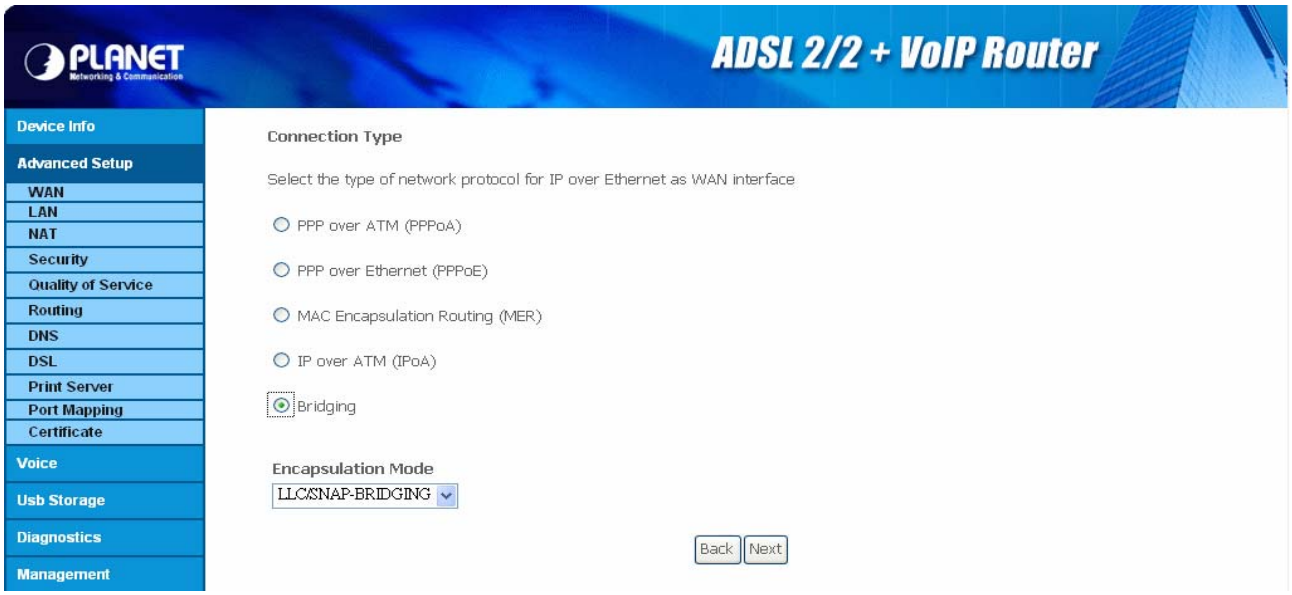


Figure: Bridge mode

Enable 802.1q: If enable it, input the 802.1q VLAN tag value. Note that 802.1q VLAN tagging is only available for PPPoE, MER and Bridge.

Click “Next” to show the following interface.

4. In this interface, you can modify the Service name.

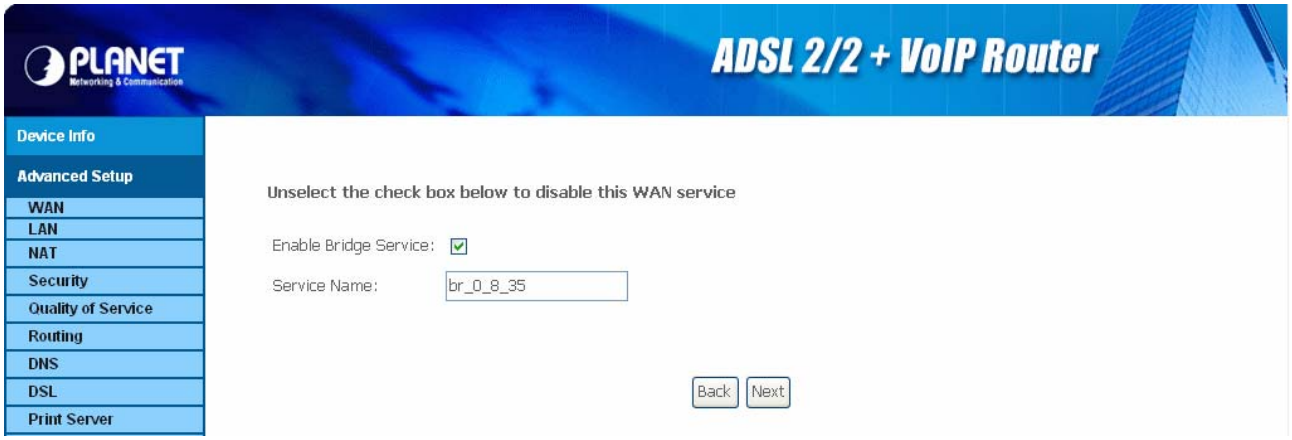


Figure: Bridge service page

WAN Service: Please enable it, unless you don’t need to active the PVC.

Click “Next” to show the following interface.

5. In this interface, it show the all configuration.

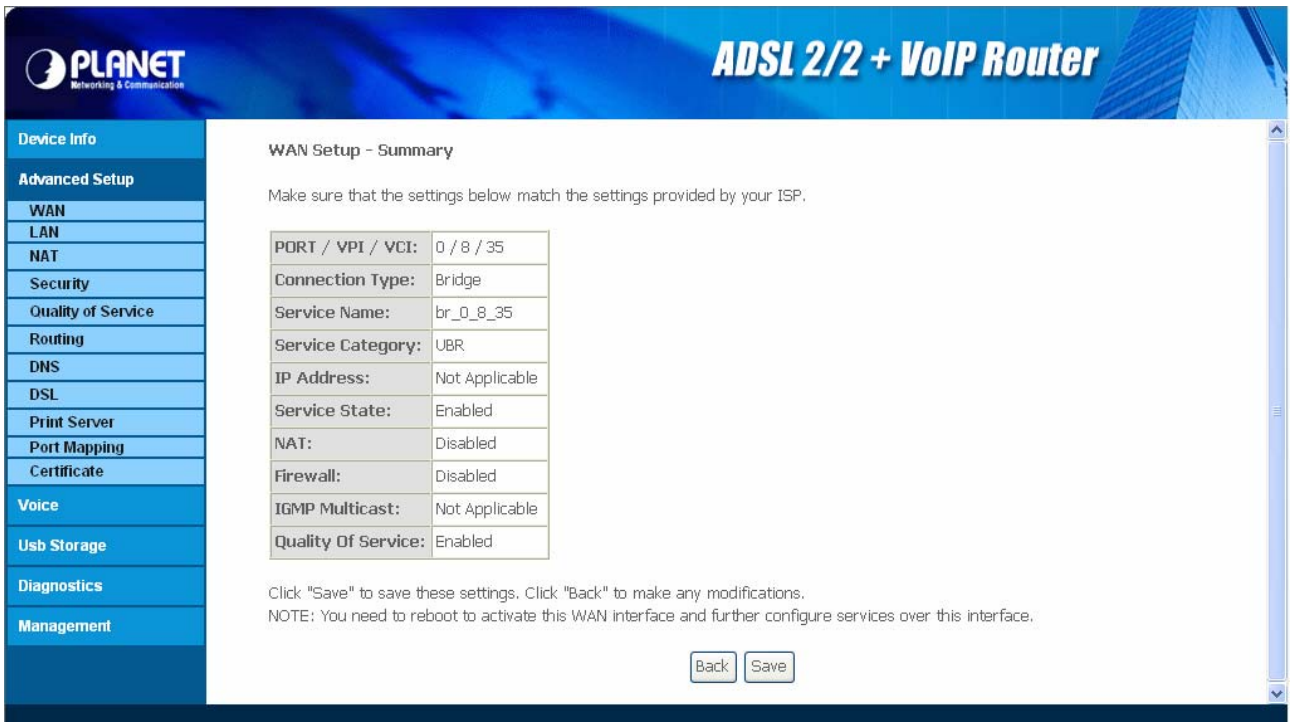


Figure: Bridge Setup Summary

Click “Save” to save these settings.And you can click “Back” to make any modifications. After you click “Save”, it show the following interface.

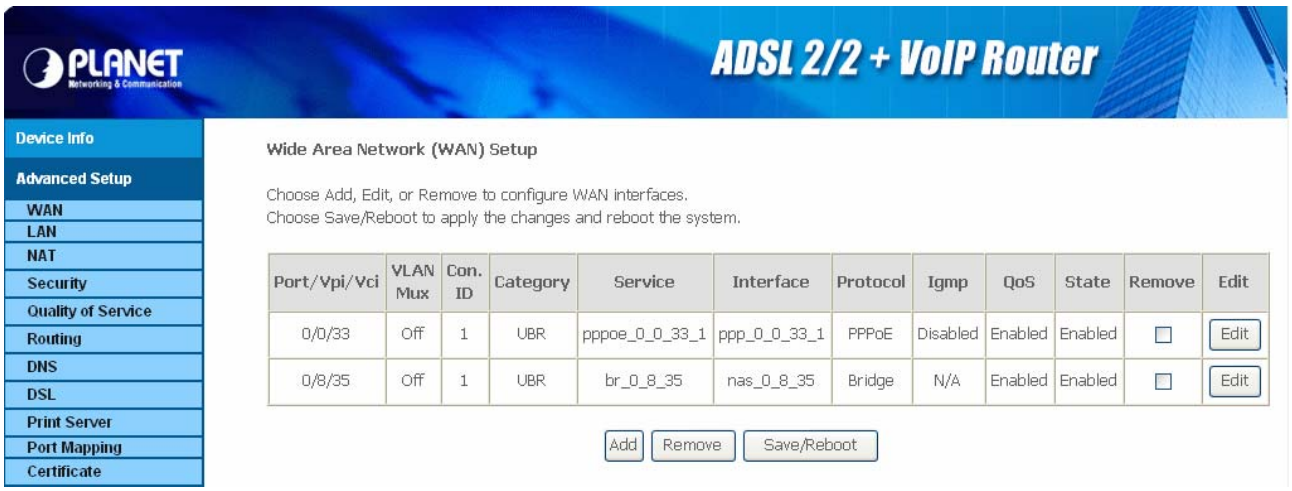


Figure: Bridge Setup Complete

NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

3.3.2 LAN configuration

You can use the LAN configuration to define an IP address for the DSL Router and configure the DHCP server

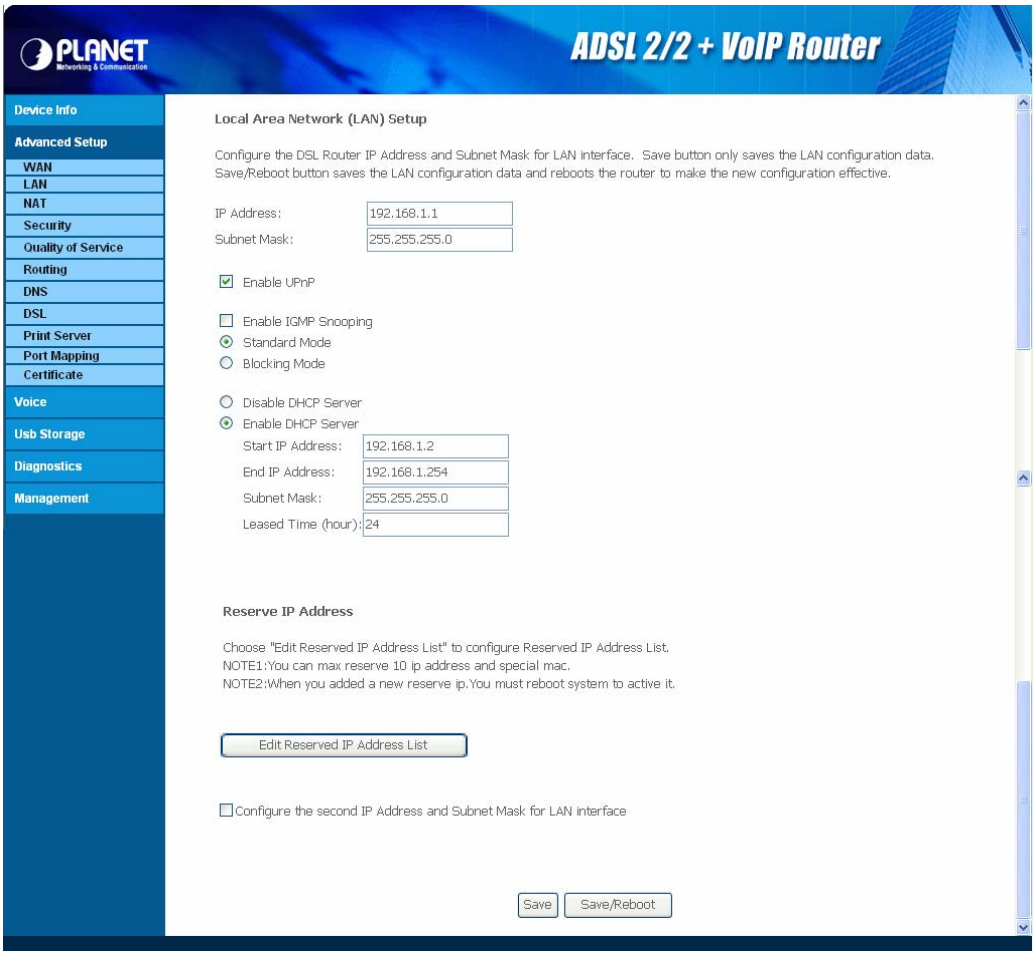


Figure: LAN configuration setup

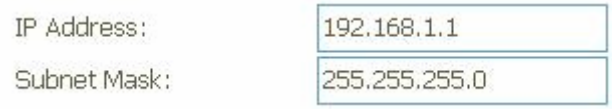
Defining the private IP address for the DSL Router

On this screen you can change the device's IP address. The preset IP address is 192.168.1.1. This is the Private IP address of the DSL Router. This is the address under which the device can be reached in the local network. It can be freely assigned from the block of available addresses.

- If you want to assign a different IP address to the DSL Router, enter it in the fields next to IP address.
- Adjust the Subnet mask if necessary.

We recommend that you use an address from a block that is reserved for private use.

This address block is 192.168.1.1-192.168.255.254



Note:

New settings can only be made after the DSL Router has been rebooted. If necessary, reconfigure the IP address on your PC (including one that is statically assigned) so that it matches the new configuration.

Enable UPNP (Universal Plug and Play)

PCs with UPnP (Universal Plug & Play) can offer their own network services and automatically use services offered in the network.

Note:

The PC must have WindowsME or WindowsXP as its operating system. Check whether the UPnP function has been installed in the PC's operating system. It may be necessary to retrospectively install the UPnP components, even on systems with WindowsXP or WindowsME. Please consult your PC's user guide.

Enable IGMP Snooping

Internet Group Management Protocol

IGMP is an Internet Protocol that enables an Internet computer to inform neighboring routers that it is a member of a multicast group. With multicasting, a computer can send content on the Internet to several other computers that have registered an interest in the first computer's content. Multicasting can, for example, be used for multimedia programs for media streaming to recipients that have set up multicast group membership.

Note:

If IGMP Snooping function is active, DSL Router capability will improve

Configuring the DHCP server

The DSL ROUTE has a DHCP server for which the factory setting is active. Consequently, the IP addresses of the PCs are automatically assigned by the DSL Router.

Note:

- If the DHCP server for the DSL Router is activated, you can configure the network setting on the PC so that the option Obtain an IP address automatically is set up. Further information about this can be found in the section entitled
- If you deactivate the DHCP server, you will have to assign a static IP address for the PCs that use the network settings

- To activate the DHCP server, select ‘Enable’.
- If the DHCP server is active, you can define a Lease time. The Lease time determines the period for which the PCs retain the IP addresses assigned to them without changing them.

Note:

If you select Never expires, the IP addresses are never changed. Activate this option if you want to make NAT or firewall settings using the IP addresses of the PCs; otherwise you have to assign static IP addresses to these PCs.

3.3.3 NAT-- Network Address Translation

Overview

Setting up the NAT function

- The DSL Router comes equipped with the NAT (Network Address Translation) function. With address mapping, several users in the local network can access the Internet via one or more public IP addresses. All the local IP addresses are assigned to the router's public IP address by default.

- One of the characteristics of NAT is that data from the Internet is not allowed into the local network unless it has been explicitly requested by one of the PCs in the network. Most Internet applications can run behind the NAT firewall without any problems. For example, if you request Internet pages or send and receive e-mails, the request for data from the Internet comes from a PC in the local network, and so the router allows the data through. The router opens precisely one port for the application. A port in this context is an internal PC address, via which the data is exchanged between the Internet and a client on a PC in the local network. Communicating via a port is subject to the rules of a particular protocol (TCP or UDP).

- If an external application tries to send a call to a PC in the local network, the router will block it. There is no open port via which the data could enter the local network. Some applications, such as games on the Internet, require several links, i.e. several ports so that the players can communicate with each other. In addition, these applications must also be permitted to send requests from other users on the Internet to users in the local network. These applications cannot be run if Network Address Translation (NAT) has been activated.

- Using port forwarding (the forwarding of requests to particular ports) the router is forced to send requests from the Internet for a certain service, e.g. a game, to the appropriate port(s) on the PC on which the game is running. Port triggering is a special variant of port forwarding. Unlike port forwarding, the DSL Router forwards the data from the port block to the PC which has previously sent data to the Internet via a certain port (trigger port). This means that approval for the data transfer is not tied to one specific PC in the network, but rather to the port numbers of the required Internet service. Where configuration is concerned, this means: You have to define a so-called trigger port for the application and also the protocol (TCP or UDP) that this port uses. You then assign the public ports that are to be opened for the application to this trigger port. u The router checks all outgoing data for the port number and protocol. If it identifies a match of port and protocol for a defined trigger

port, then it will open the assigned public ports and notes the IP address of the PC that sent the data. If data comes back from the Internet via one of these public ports, the router allows it through and directs it to the appropriate PC. A trigger event always comes from a PC within the local network. If a trigger port is addressed from outside, the router simply ignores it.

Note:

- An application that is configured for port triggering can only be run by one user in the local network at a time.
- As long as the public ports are open, they can be used by unauthorized persons to gain access to a PC in the local network.

When the DSL Router is supplied, the NAT function (Network Address Translation) is activated, i.e. all IP addresses of PCs in the local network are converted to the router's public IP address when accessing the Internet. You can use the NAT settings to configure the DSL Router to carry out the following tasks:

Note:

For the functions described below, the IP addresses of the PCs must remain unchanged. If the IP addresses of the PCs are assigned via the DHCP server of the DSL Router, you must select Never expires (see page79) as the settings in the Local Network menu entry for the Lease time or assign static IP addresses for the PCs.

You can activate or deactivate the NAT function (by default the NAT function is activated).

3.3.3.1 NAT -- Virtual Servers Setup

In its default state, DSL router blocks all external users from connecting to or communicating with your net-work. Therefore the system is safe from hackers who may try to intrude on the network and damage it. However, you may want to expose your network to the Internet in certain limited and controlled ways in order to enable some applications to work from the LAN (game, voice and chat applications, for example) and to enable Internet-access to servers in the home network. The Port Forwarding feature supports both of these functionalities. If you are familiar with networking terminology and concepts, you may have encountered this topic referred to as “Local Servers” The Port Forwarding screen lets you define the applications that require special handling by DSL router .All you have to do is select the application protocol and the local IP address of the computer that will be using or providing the service. If required, you may add new protocols in addition to the most common ones provided by DSL router. For example, if you wanted to use a File Transfer Protocol (FTP) application on one of your PCs, you would simply select FTP from the list and enter the local IP address or host name of the designated computer. All FTP-related data arriving at DSL router from the Internet will henceforth be forwarded to the specific computer. Similarly, you can grant Internet users access to servers inside your home network, by identifying each service and the PC that will provide it. This is useful, for example, if you want to host a Web server inside your home network. When an Internet user points his/her browser to DSL router external IP address, the gateway will forward the incoming HTTP request to your Web server. With one external IP address (DSL router main IP address), different applications can be assigned to your LAN computers, however each type of application is limited to use one computer. For example, you can de net hat FTP will use address X to reach computer A and Telnet will also use address X to reach computer A, but attempting to define FTP to use address X to reach both computer A and B will fail. DSL router therefore provides the ability to add additional public IP addresses to port forwarding rules, which you must obtain from your ISP, and enter into the NT IP Addresses Pool (see section 7.3.7). You will then be able to define FTP to use address X to reach computer A and address Y to reach computer B. Additionally, port forwarding enables you to redirect traffic to a different port instead of the one to which it was designated. Lets say, that you have a Web server running on your PC on port 8080 and you want to grant access to this server to any one who accesses DSL router via HTTP To accomplish this, do the following:

- Define a port forwarding rule for the HTTP service, with the PC IP or host name.
- Specify 8080 in the Forward to Port’ field.

All incoming HTTP traffic will now be forwarded to the PC running the Web server on port 8080 when setting a port forwarding service; you must ensure that the port is not already in use by another application, which may stop functioning. A common example is when using SIP signaling in Voice over IP the port used by the gateway VoIP application (5060) is the same port on which port forwarding is set for LAN SIP agents.

Note:

Some applications, such as FTP, TFTP, PPTP and H323, require the support of special specific Application Level Gateway (ALG) modules in order to work inside the home network. Data packets associated with these applications contain information that allows them to be routed correctly. An ALG is needed to handle these packets and ensure that they reach their intended destinations. DSL router is equipped with a robust list of ALG modules in order to enable maximum functionality in the home network The ALG is automatically assigned based on the destination port

Add Port Forwarding

- To set up Virtual Servers for a service, select the Advanced Setup → NAT → Virtual Servers and click “add” to add the Virtual Server.

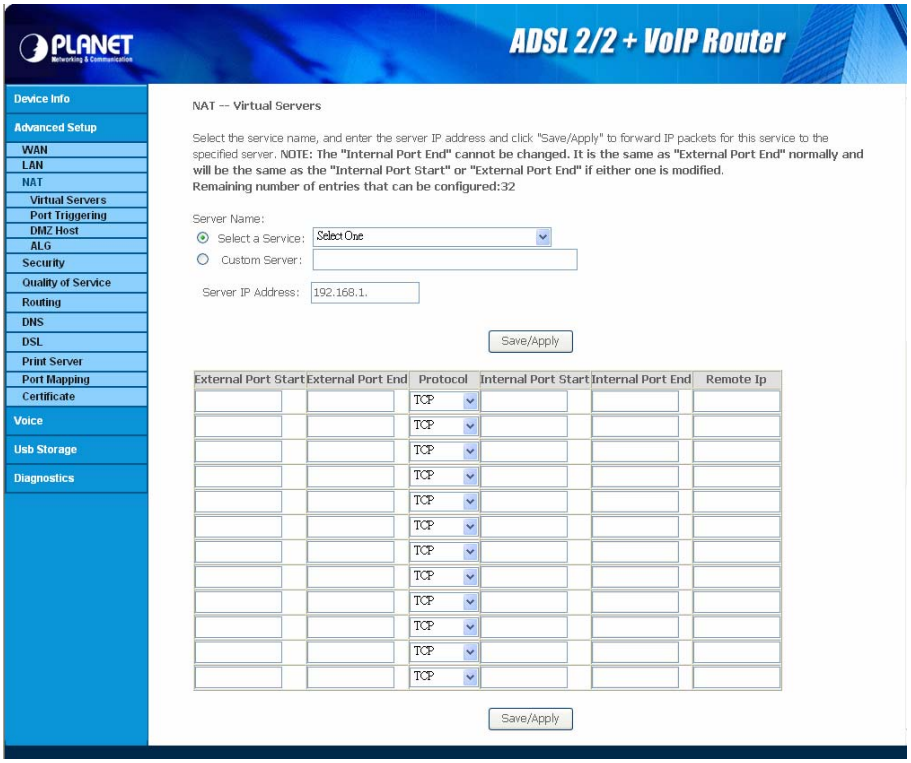


Figure: Add virtual Servers

- Select a service ,or custom your server
- Set Server IP address
- Enter the Set Server IP address of the computer that will provide the service (the server in the Local Host field. Note that unless an additional external IP address has been added, only one LAN computer can be assigned to provide a specific service or application.
- Set External port start external port end
- Select protocol
- Set Internal port start and internal port end

- Entry Remote IP
- Click OK to apply the settings

If the application you require is not in the list, you must manually enter the relevant data on the screen:

Select the protocol for the service you are providing from the Protocol list. Under Public port, enter the port number of the service you are providing. In the Local port field, enter the internal port number to which service requests are to be forwarded. In the Local IP address field, enter the IP address of the PC that provides the service.

Example: the Web server has been configured to react to requests on port 8080. However, the requests from websites enter the Web server via port 80 (standard value). If you add the PC to the forwarding table and define port 80 as the public port and port 8080 as an internal port, all requests from the Internet are diverted to the service with the port number 80 on the Web server of the PC you have defined with port 8080.

Note:

You can use a single port number, several port numbers separated by commas, port blocks consisting of two port numbers separated by a dash, or any combination of these, for example 80, 90-140, 180.

Del Port Forwarding

- Click remove box
- Click remove to apply the settings

3.3.3.2 Port Triggering

If you configure port triggering for a certain application, you need to determine a so-called trigger port and the protocol (TCP or UDP) that this port uses. You then assign the public ports that are to be opened for the application to this trigger port. You can select known Internet services or assign ports or port blocks manually.

Add port Triggering

To set up port triggering for a service, select Port Triggering from the Advanced

- Settings → NAT → Port Triggering → add

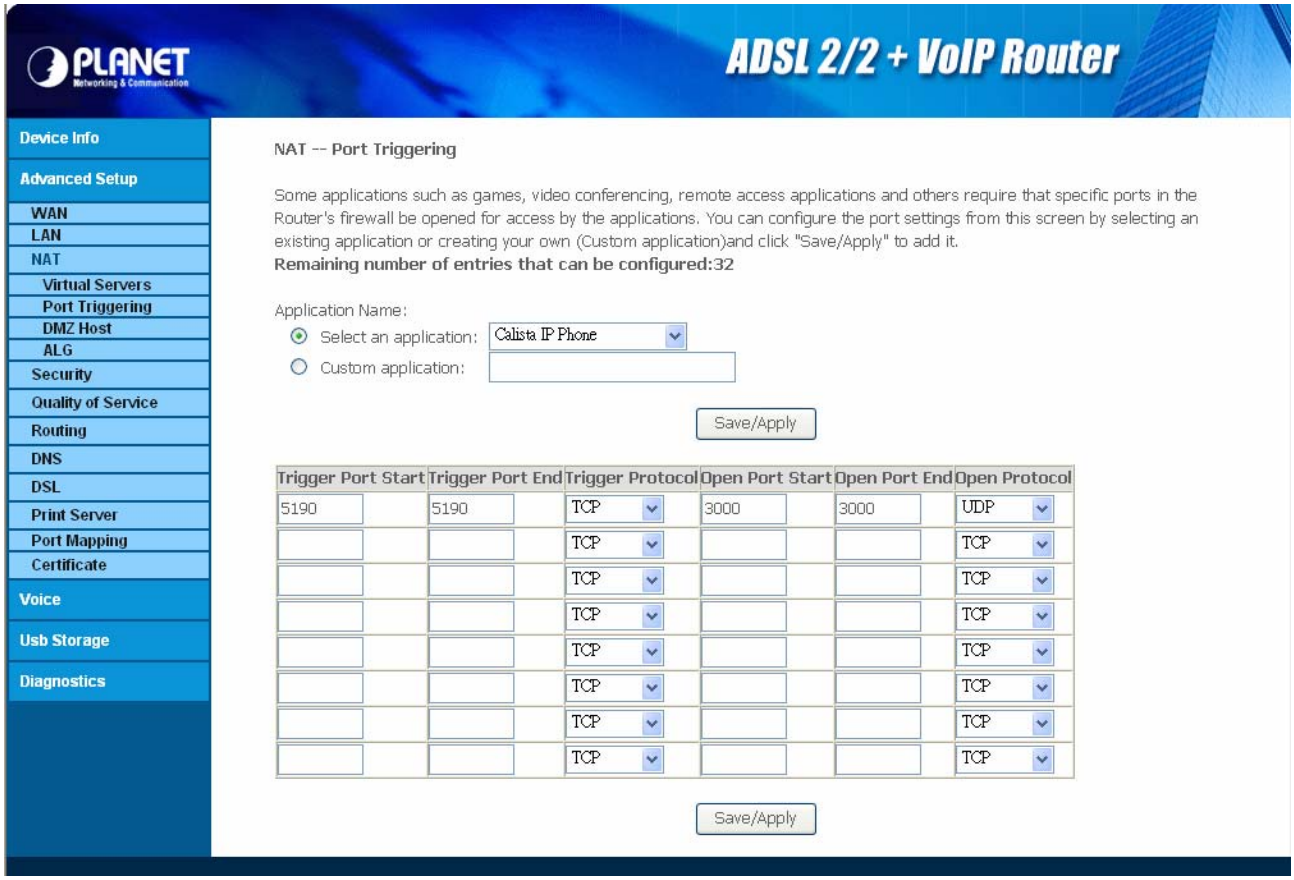


Figure: Port Triggering

- Select the required application from the applications list.

  If the application you require is not in the list, you must enter the relevant data on the screen custom application
- Trigger port start and Trigger port end: Enter the port that is to be monitored for outgoing data traffic.
- Trigger protocol: Select the protocol that is to be monitored for outgoing data traffic.
- Open Protocol: Select the protocol that is to be allowed for incoming data traffic
- Open port start and Open port end: Enter the port that is to be opened for incoming traffic.

Note:

You can use a single port number, several port numbers separated by commas, port blocks consisting of two port numbers separated by a dash, or any combination of these, for example 80, 90-140, 180.

- Apply the settings by clicking “save/apply”

Remove port Triggering

Check remove box

Apply setting by click Save/Apply

3.3.3.3 DMZ Host

The DMZ (Demilitarized) Host feature allows one local computer to be exposed to the Internet. You wish to use a special-purpose Internet service, such as an on-line game or video-conferencing Program, that is not present in the Port Forwarding list and for which no port range information is available. You are not concerned with security and wish to expose one computer to all services without restriction.

Note:

A DMZ host is not protected by the firewall and may be vulnerable to attack. Designating a DMZ host may also put other computer sin the home net work at risk. When using a DMZ host, you must consider the security implications and protect it if necessary.

You can set up a client in your local network to be a so-called "DMZ host". Your device will then forward all incoming data traffic from the Internet to this client. You can then, for example, operate your own Web server on one of the clients in your local network and make it accessible to Internet users. As the exposed host, the local client is directly visible to the Internet and therefore particularly vulnerable to attacks (e.g. hacker attacks). Only activate this function if it is absolutely necessary (e.g. to operate a Web server) and other functions (e.g. port forwarding) are not adequate. In this case you should take appropriate measures for the clients concerned.

Note:

Only one PC per public IP address can be set up as an Exposed Host

Add a DMZ host

- To set up a PC as an DMZ host, select DMZ Host from the Advanced Setup→NAT→ DMZ host

PLANET
Networking & Communication
ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
WAN
LAN
NAT
Virtual Servers
Port Triggering
DMZ Host
ALG
Security
Quality of Service
Routing
NAT -- DMZ Host
The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.
Enter the computer's IP address and click "Apply" to activate the DMZ host.
Clear the IP address field and click "Apply" to deactivate the DMZ host.
DMZ Host IP Address:
192.168.1.10
Save/Apply

Figure: DMZ Host Config

- Enter the Local IP address of the PC that is to be enabled as an Exposed Host.
- Apply the settings by clicking “Save/Apply”.

Remove DMZ host

Clear the DMZ Host Address

Apply setting by click **Save/Apply**

3.3.4 Security

Security is an important function of DSL; it protects the resources of a private network from users from other networks. Also the item prevents unauthorized internet users form accessing private networks connected to the internet. All messages entering or leaving the intranet (i.e., the local network to which you are connected) must pass through the security examines, which examines each message and blocks those that do not meet the specified security criteria.

There are three basic types of security techniques:

- IP packet filtering: The system examines each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure.
- Circuit-level gateway implementation: This process applies security mechanisms when a TCP or UDP connection is established. Once the connect has been made, packets can flow between the hosts without further checking.
- MAC frame filtering: The system examines each frame entering or leaving the network form layer 2. And accord to user-defined rules accepts and rejects frame.

A security management program can be configured one of two basic ways:

- A default-deny policy.
- A default-allow policy.

A default-deny approach to security is by far the more secure, but due to the difficulty in configuring and managing a network in that fashion, many networks instead use the default-allow approach. Let's assume for the moment that your security management program utilizes a default-deny policy, and you only have certain services enabled that you want people to be able to use from the Internet.

NOTE: The security is like a firewall.

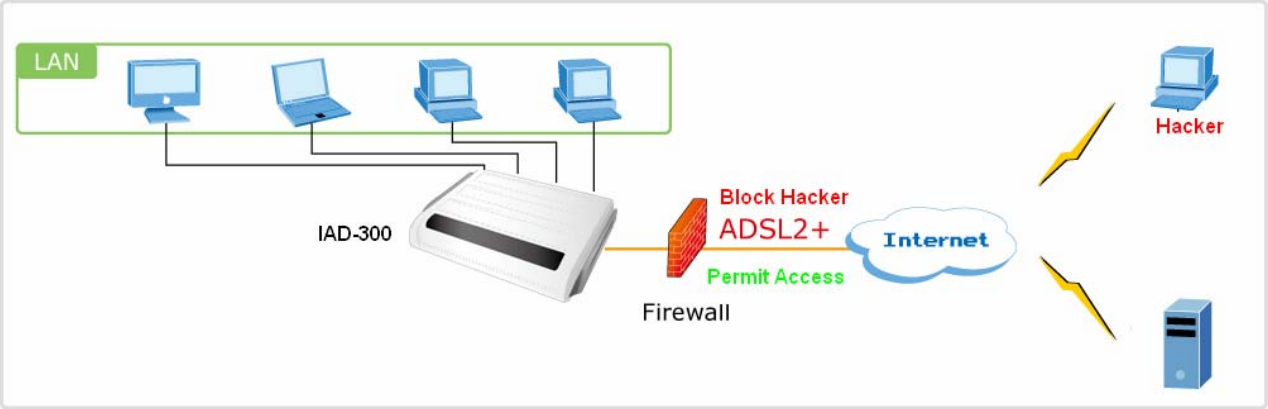


Figure: the Security application

Click “Security” -->” IP Filtering” to show the following interface. By default, the firewall is enabled. The firewall is used to block document transmissions between the Internet and your PC. It serves as a safety guard and only permits authorized documents to be sent into the LAN.

Note: If the Router configured as **bridge mode**, the **IP Filtering** will **disabled** and the IP filtering interface will disappear.

And if the Router configured as **Non-Bridge mode** PVC, the **MAC Filtering** will disabled and the MAC Filtering interface will disappear.

3.3.4.1 Outgoing IP Filtering Setup

When Outgoing IP Filtering rules setup being enable on the ROUTER, the various security functions for the local network will enable at the same time .You can protect the network against hacker attacks and block individual PC's access to selected services or internet sites.

Click "Security"-->" IP Filtering"-->" Outgoing" to show the following interface.

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters.

Figure: Outgoing IP Filtering Config

Click "Add" to enter the related interface defining the IP filtering rule as follows.

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

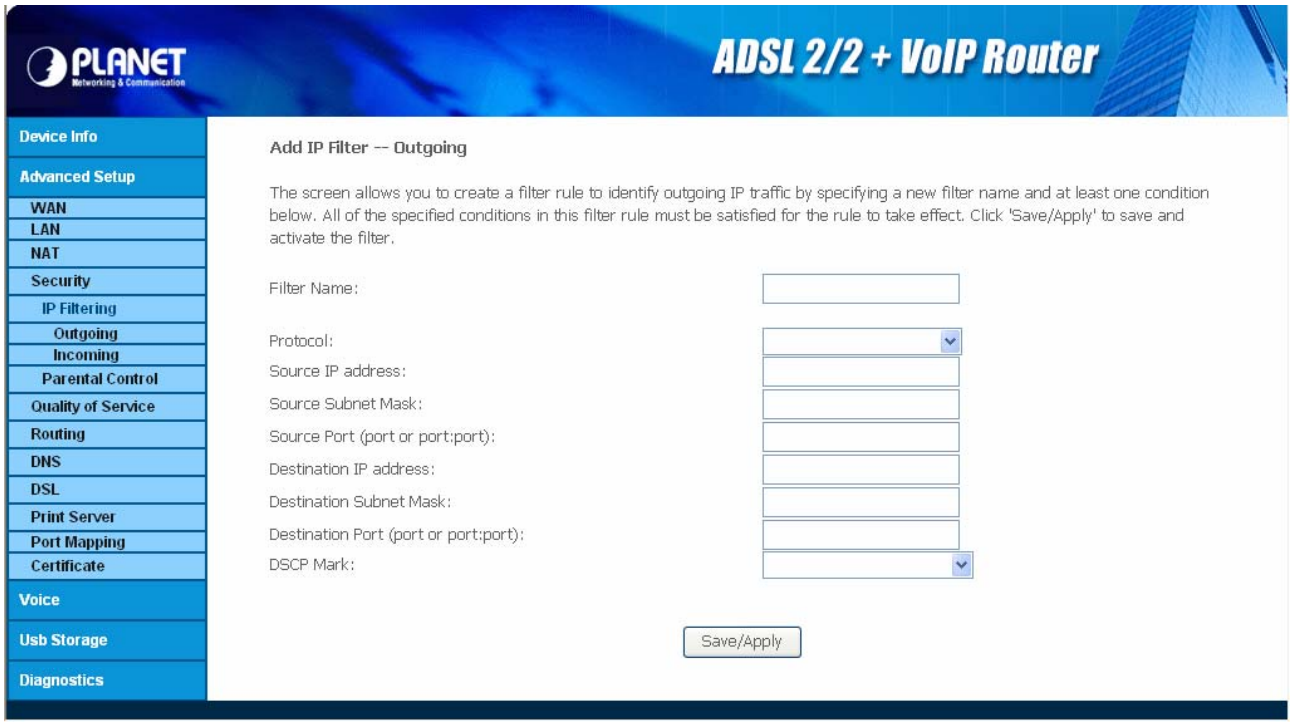


Figure: Outgoing IP Filtering Add Setup

- Filter Name: Enter the name of outgoing filter rule
- Protocol: Select one among TCP/UDP TCP UDP or ICMP protocols
- Source IP address: Enter an IP address. When you have set IP address, the outgoing packet (protocol selected packet) will block.
- Source subnet mask
- Source port : UPD/TCP source port or a range of ports
- Destination IP address: Destination IP (default no set)
- Destination subnet mask:
- Destination port : UPD/TCP destination port or a range of ports

There is an example to introduce how to configure the outgoing IP Filtering.

The topology is as follows:

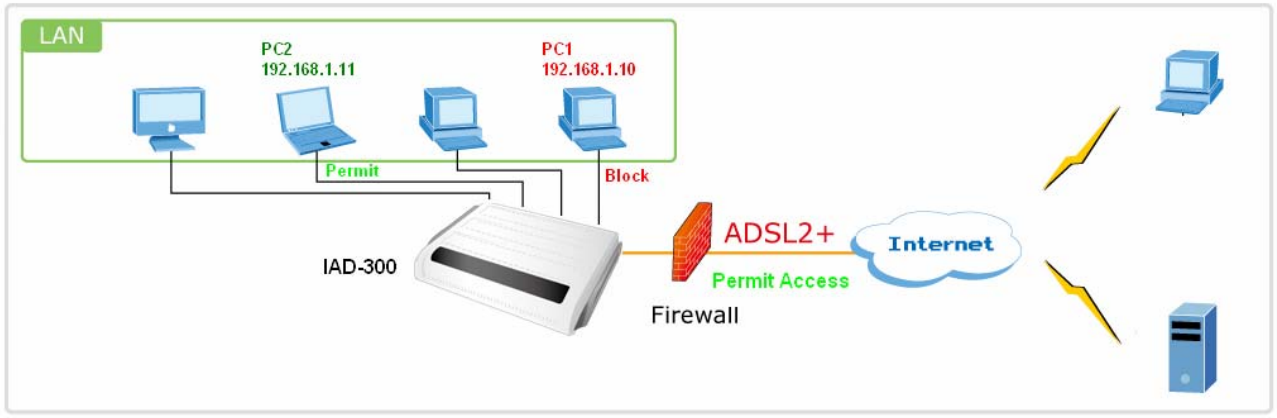


Figure: Outgoing IP filer application

Request:

- I need to block a whose IP address is 192.168.1.10. All outgoing UDP/TCP packet from that PC1(192.168.1.10) is disallowed.
- Allow all outgoing traffic packet from PC2 (192.168.1.11).

Configuration:

1. By default, all outgoing IP traffic from LAN is allowed, so allow all the IP packet come for the PC2.
2. The detailed configuration steps are as follows:

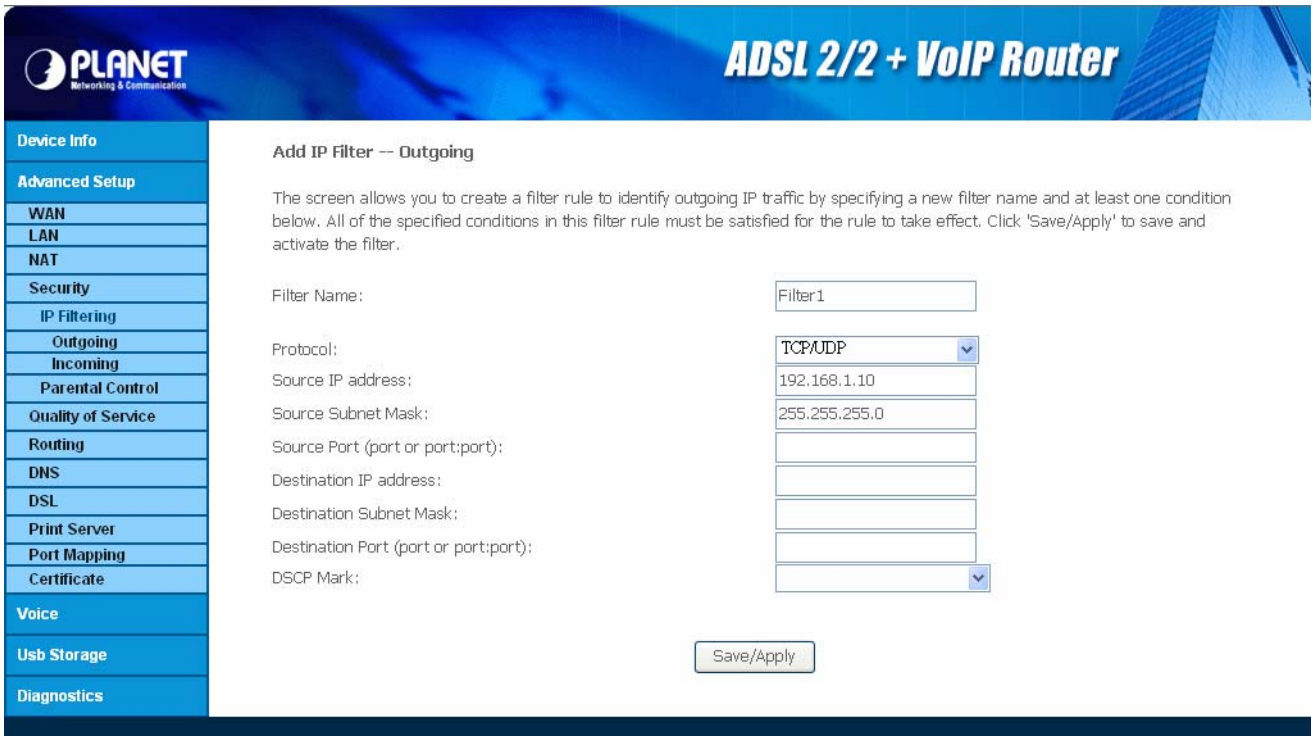


Figure: Outgoing IP Filtering Add Setup example

3. Click “Save/apply” to show below.

Figure: Outgoing IP Filtering Config Complete

3.3.4.2 Incoming IP Filtering Setup

The incoming IP filter is used to block and permit IP packet transmisstion from internet. By default incoming IP filter block all incoming packet from internet. When incoming IP Filtering rules setup being enable on the ROUTER, you can permit remote individual PC to access various local network service .

Click “Security”-->” IP Filtering”-->” Incoming” to show the following interface.

By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be ACCEPTED by setting up filters.

Figure: Incoming IP Filtering Config

Click “Add” to enter the related interface defining the IP filtering rule as follows.

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

And you must select at least one or multiple WAN interfaces to apply this rule.

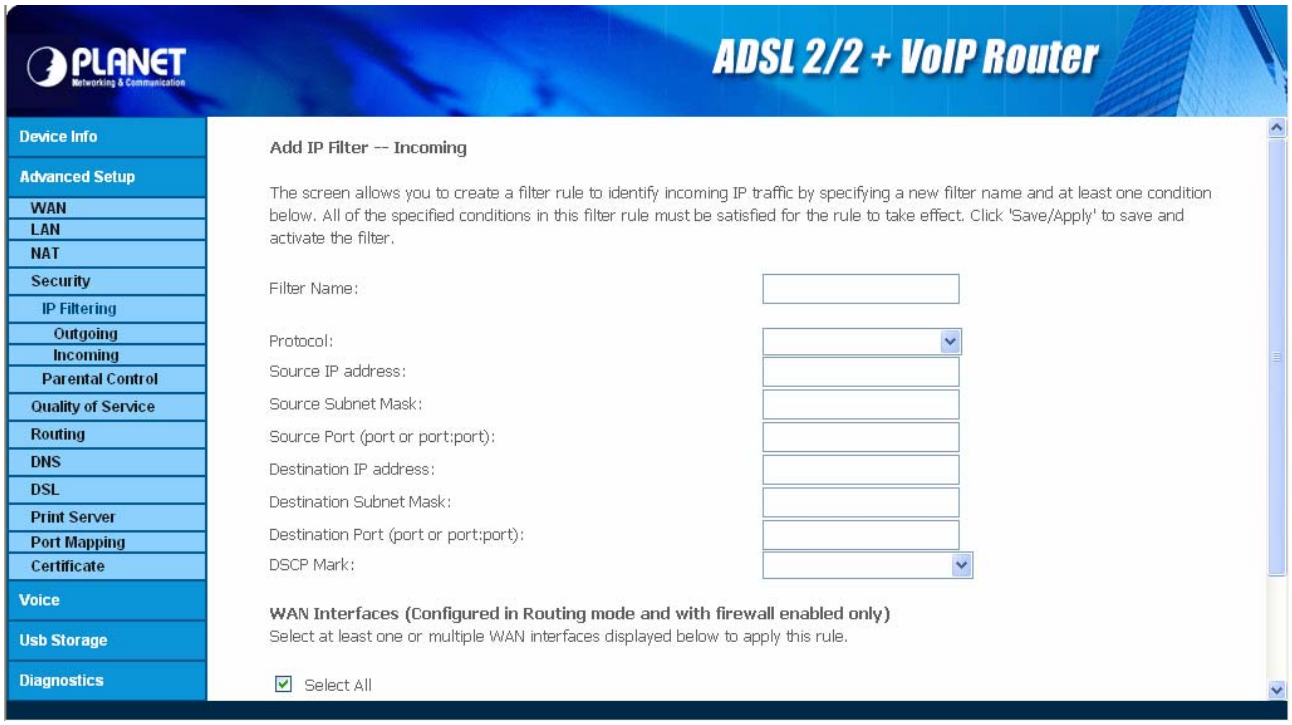

PLANET
ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
IP Filtering
Outgoing
Incoming
Parental Control
Quality of Service
Routing
DNS
DSL
Print Server
Port Mapping
Certificate
Voice
Usb Storage
Diagnostics
Add IP Filter -- Incoming
The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.
Filter Name:
Protocol:
Source IP address:
Source Subnet Mask:
Source Port (port or port:port):
Destination IP address:
Destination Subnet Mask:
Destination Port (port or port:port):
DSCP Mark:
WAN Interfaces (Configured in Routing mode and with firewall enabled only)
Select at least one or multiple WAN interfaces displayed below to apply this rule.
Select All

Figure: Incoming IP Filtering Add Setup

- Filter Name: Enter the name of incoming filter rule
- Protocol: Select one among TCP/UDP TCP UDP or ICMP protocols
- Source IP address: Enter an IP address. When you have set IP address, the incoming packet (protocol selected packet) will allow.
- Source subnet mask:
- Source port : UPD/TCP source port or a range of ports
- Destination IP address: Destination IP (default no set)
- Destination subnet mask:
- Destination port : UPD/TCP destination port or a range of ports
- Wan interfaces: You can select WAN interfaces and PVC

There is an example to introduce how to configure the incoming IP Filtering:

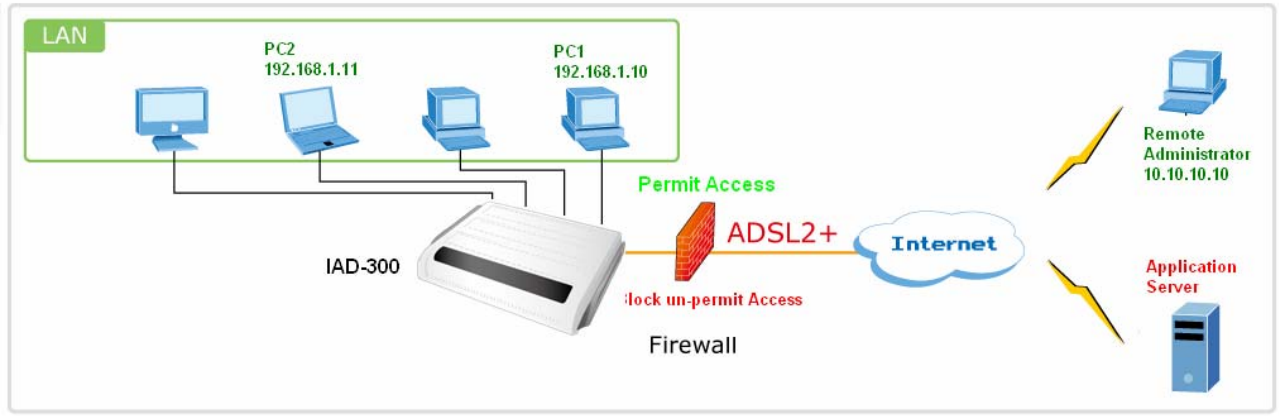


Figure: incoming IP filer application

Request:

- I need to permit a PC whose IP address is 10.10.10.10. All Incoming TCP/UDP packet traffic from that PC(10.10.10.10) is allowed.
- Block all IP traffic from other PC .

Configuration:

1. By default, all incoming IP traffic from internet is blocked, so all the IP packets come for the internet are blocked.
2. The detailed configuration steps are as follows:

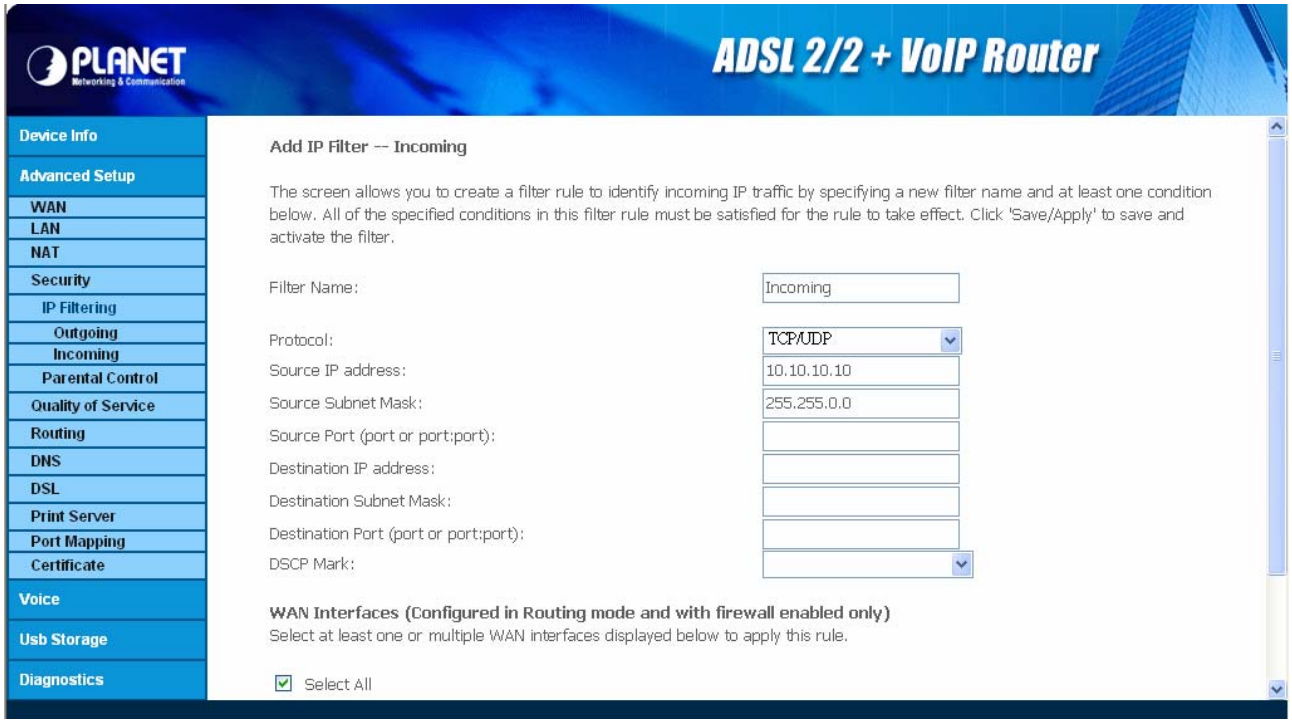


Figure: Incoming IP Filtering Add Setup example

3. Click “Save/apply” to show below.

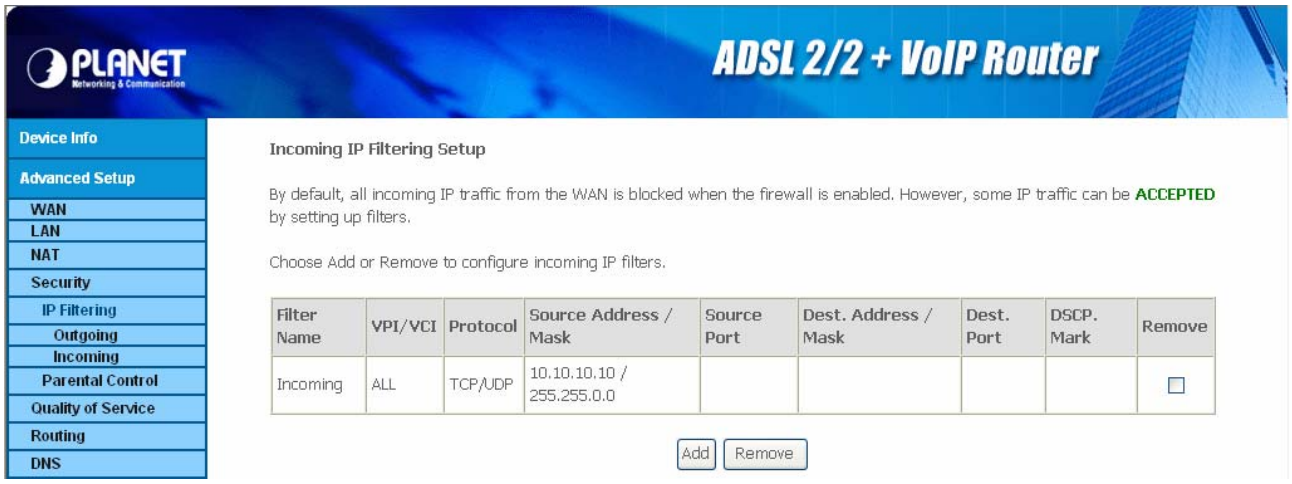


Figure: Incoming IP Filtering Config Complete

3.3.4.3 MAC Filtering Setup

May be you want manage Layer 2 MAC address to block or permit a computer within the home network .when you enable MAC filter rules ,the ROUTER serves as a firewall which work at layer 2.

Click “Security”-->”MAC Filtering” to show the following interface.

Note: MAC Filtering is only effective on ATM PVCs configured in Bridge mode. If the ATM PVCs is configured in other routing mode(such as PPPoE mode), the “MAC Filtering Setup” will not appears in the “Security” option.

FORWARDED means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

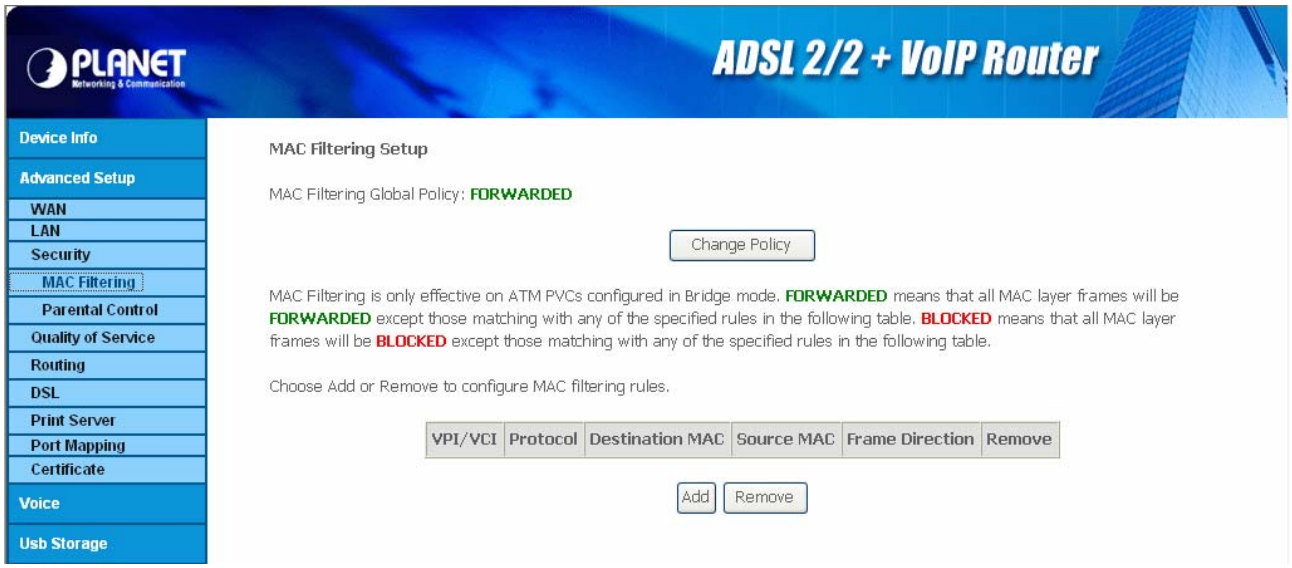


Figure: MAC Filtering Setup overview

Click “Change Policy” to show the following interface. Then you can change the MAC Filtering Global Policy from FORWARDED to BLOCKED.

PLANET
ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
WAN
LAN
Security
MAC Filtering
Parental Control
Quality of Service
Routing
Change MAC Filtering Global Policy
WARNING: Changing from one global policy to another will cause all defined rules to be REMOVED AUTOMATICALLY!
You will need to create new rules for the new policy.
Are you sure you want to change MAC Filtering Global Policy from FORWARDED to BLOCKED ?
NO
YES

Figure: MAC Filtering Change Policy

Click “add” to add MAC filter rules. The interface shows below.

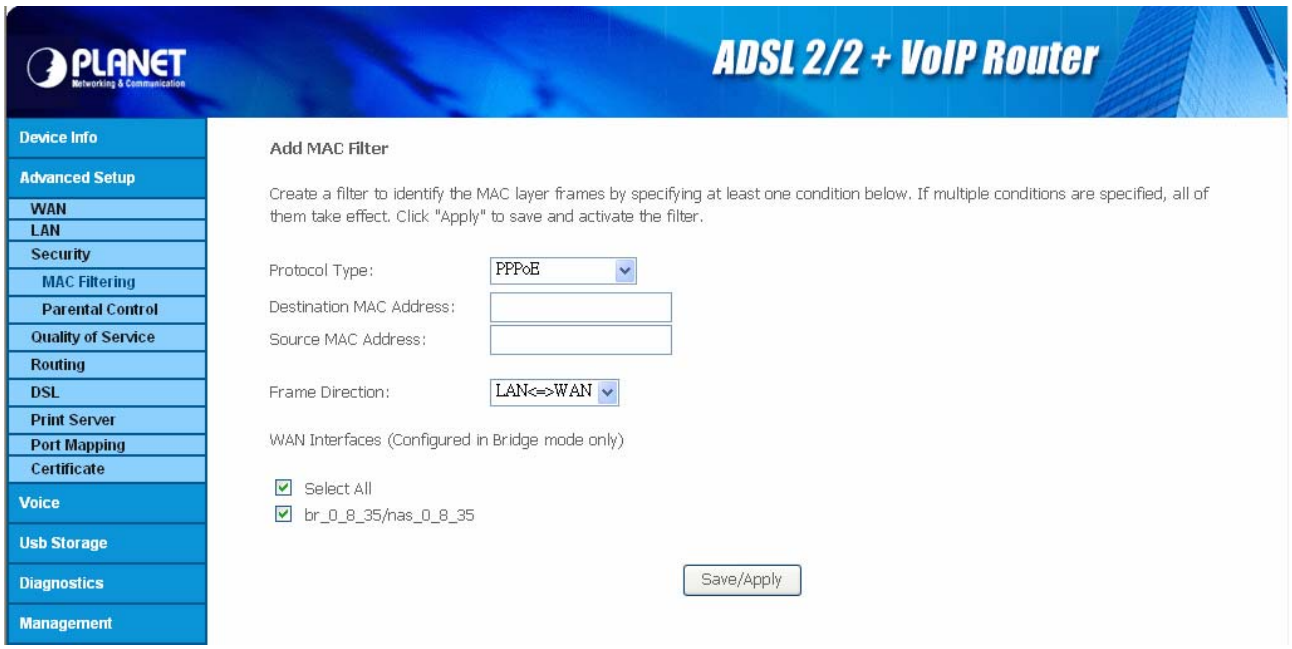


Figure: MAC Filtering Add Config

- Protocol Type: Select one among PPPoE IPV4 IPV6 AppleTalk IPX NETBEUI or ICMP protocols
- Destination MAC Address:
- Source MAC Address：
- Frame Direction: The direction of transmit frame, you can select LAN->WAN (from LAN to WAN) WAN -> LAN (from WAN to LAN) LAN ⇔ WAN.
- WAN Interface: Select a WAN interface.

3.3.5 Quality of Service

Many communication and multimedia applications require large, high speed bandwidths to transfer data between the local network and the internet. However, for many applications there is often only one internet connection available with limited capacity. QOS (Quality of Service) divides this capacity between the different applications and provides underplayed, continuous data transfer where data packets with higher priority are given preference.

Click “Quality of Service” to show the following interface. Under “Quality of Service”, there are two network share mode:” Queue Config”, ”Qos Classification”.

Quality of Service (QoS) for networks is an industry-wide set of standards and mechanisms for ensuring high-quality performance for critical applications. By using QoS mechanisms, network administrators can use existing resources efficiently and ensure the required level of service without reactively expanding or over-provisioning their networks.

Traditionally, the concept of quality in networks meant that all network traffic was treated equally. The result was that all network traffic received the network’s best effort, with no guarantees for reliability, delay, variation in delay, or other performance characteristics. With best-effort delivery service, however, a single bandwidth-intensive application can result in poor or unacceptable performance for all applications. The QoS concept of quality is one in which the requirements of some applications and users are more critical than others, which means that some traffic needs preferential treatment.

3.3.5.1 Enable QOS

In this interface, you can do QOS queue management configuration. By default ,the system is enable QOS and set a default DSCP mark to automatically mark incoming traffic without reference to particular classifier.

Click”Advance Setup”→”Quality of Classification” to show following interface:

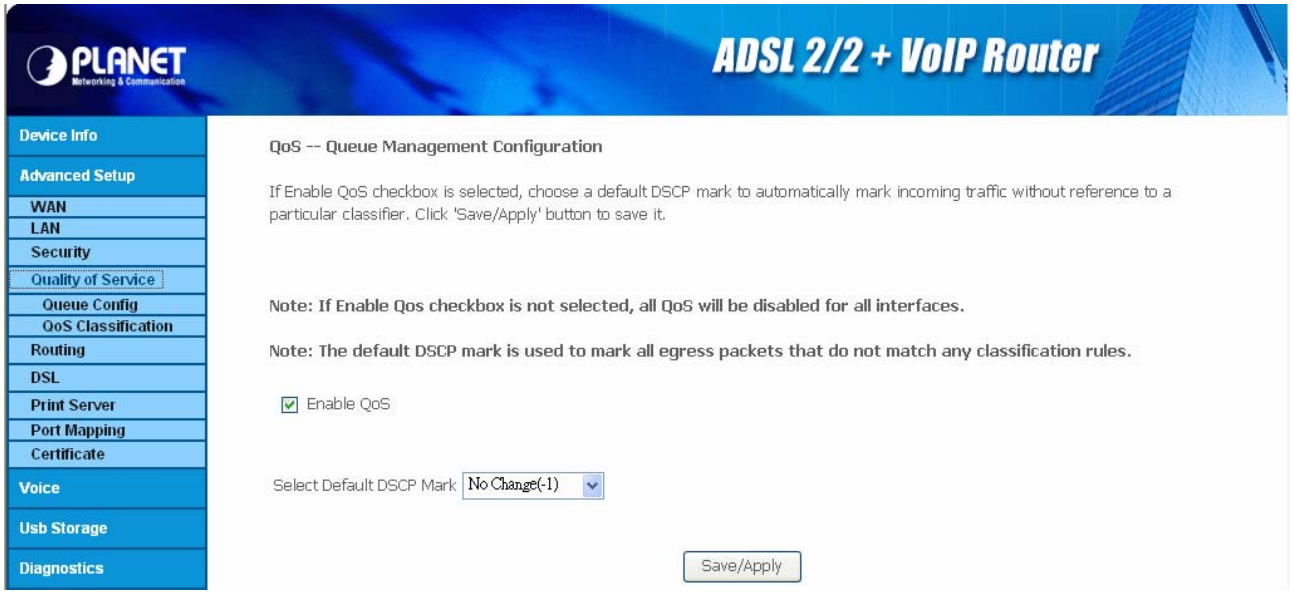

PLANET
Networking & Communication
ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
WAN
LAN
Security
Quality of Service
Queue Config
QoS Classification
Routing
DSL
Print Server
Port Mapping
Certificate
Voice
Usb Storage
Diagnostics
QoS -- Queue Management Configuration
If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Save/Apply' button to save it.
Note: If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces.
Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.
Enable QoS
Select Default DSCP Mark
No Change(-1)
Save/Apply

Figure: QOS queue management configuration

Choose “Enable QOS” can enable QOS and the system can set default DSCP mark

Click “save/Apply” to active QOS.

3.3.5.2 QOS--Queue Config

The queuing in packet QOS will become effective only when packet is forwarded to QoS-enabled PVC. Packet forwarding is determined by IP routing or bridging, not under control of the packet Qos.

Click “Queue Config” to pop up an interface as below. In this interface, you can configure QOS Queue. A maximum 24 entries can be configured.

Qos Queue Configuration can allocated three queues .Each of the queues can be configured for a precedence value (Lower integer values for precedence imply higher priority for this queue relative to others). The queue entry configured here will be used by the classifier to place ingress packets appropriately.

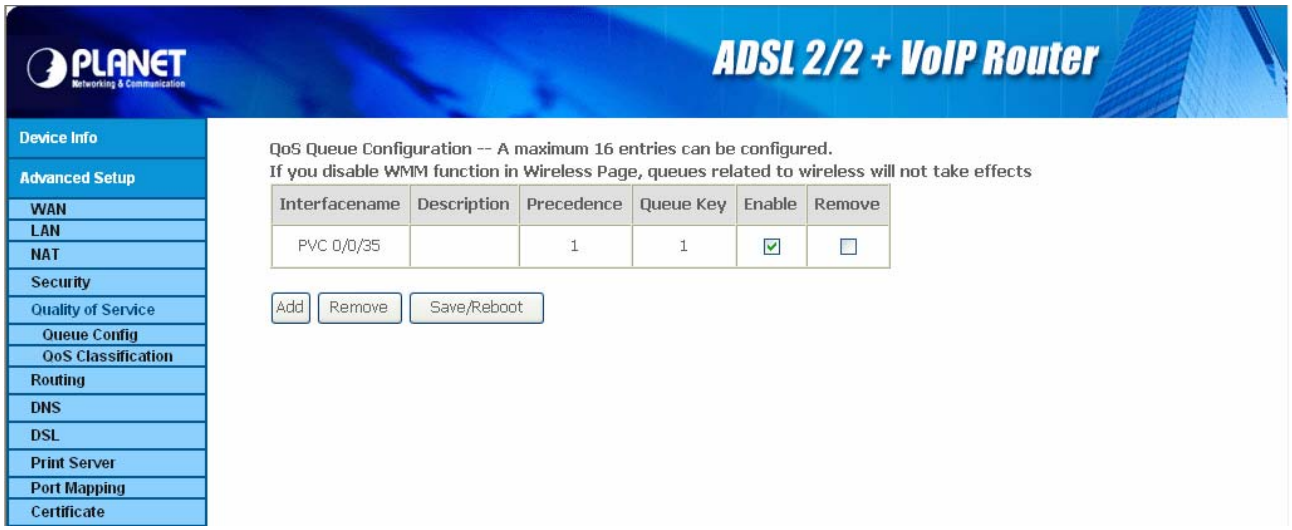


Figure2.8.8.4:QoS Queue Config overview

NOTE:

Lower integer values for precedence imply higher priority for this queue relative to others.

For example: add a Qos queue entry and allocate it to a specific network interface (PVC 0/8/81) ◦ Set integer values for queue precedence are 2.

Step 1. Click “add ” bottom to show following interface:

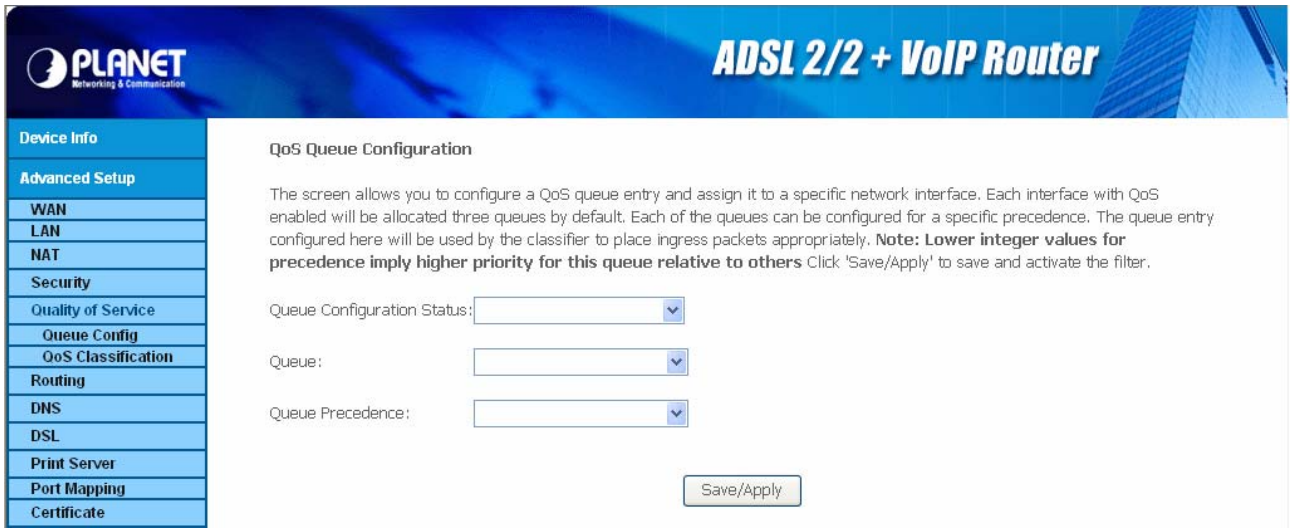

PLANET
ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Queue Config
QoS Classification
Routing
DNS
DSL
Print Server
Port Mapping
Certificate
QoS Queue Configuration
The screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each interface with QoS enabled will be allocated three queues by default. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately. Note: Lower integer values for precedence imply higher priority for this queue relative to others Click 'Save/Apply' to save and activate the filter.
Queue Configuration Status:
Queue:
Queue Precedence:
Save/Apply

Figure: QoS Queue Config

- Queue Configuration Status: Enable or Disable to configure a Qos queue entry.
- Queue : select a specific network interface. When you have already selected a network interface, the specific network interface selected will automatically allocate to the queue
- Queue Precedence: select a integer value for queue precedence. When you have already selected a integer value, the queue entry will place to ingress packets appropriately. Lower integer values for precedence imply higher priority for this queue relative to others.

Step 2. Add a Qos queue entry and assign it to a specific network interface (PVC 0/8/81), set integer values for queue precedence is 2. Show following interface:

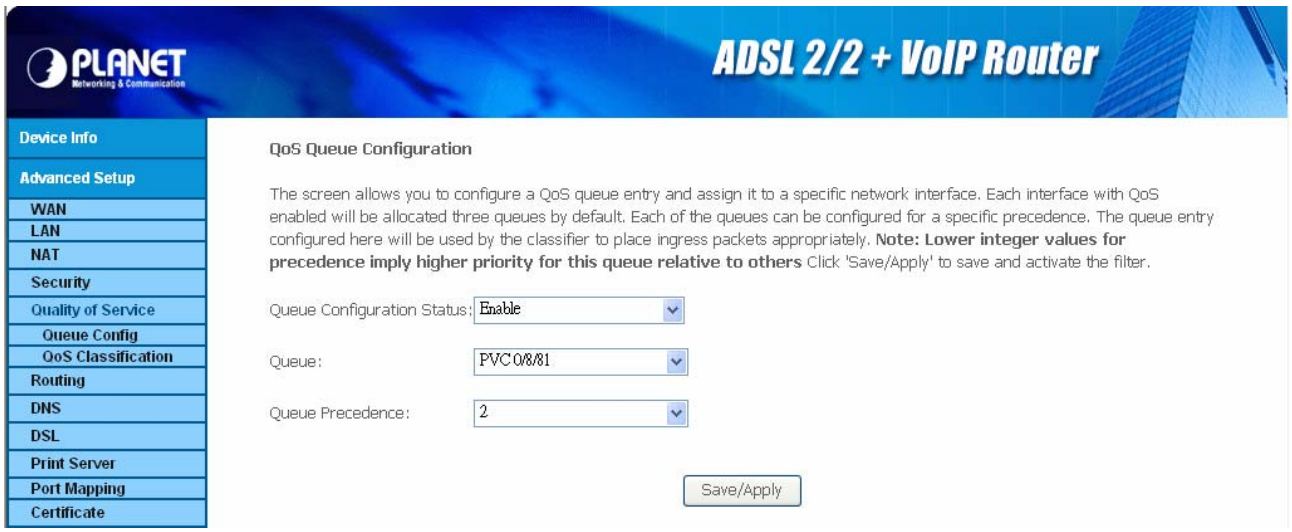

PLANET
ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Queue Config
QoS Classification
Routing
DNS
DSL
Print Server
Port Mapping
Certificate
QoS Queue Configuration
The screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each interface with QoS enabled will be allocated three queues by default. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately. Note: Lower integer values for precedence imply higher priority for this queue relative to others Click 'Save/Apply' to save and activate the filter.
Queue Configuration Status: Enable
Queue: PVC 0/8/81
Queue Precedence: 2
Save/Apply

Figure: QoS Queue Config example

Step 3. After proper modifications, click “Save/Apply” to show the following interface. (This configuration will take effective at once.)

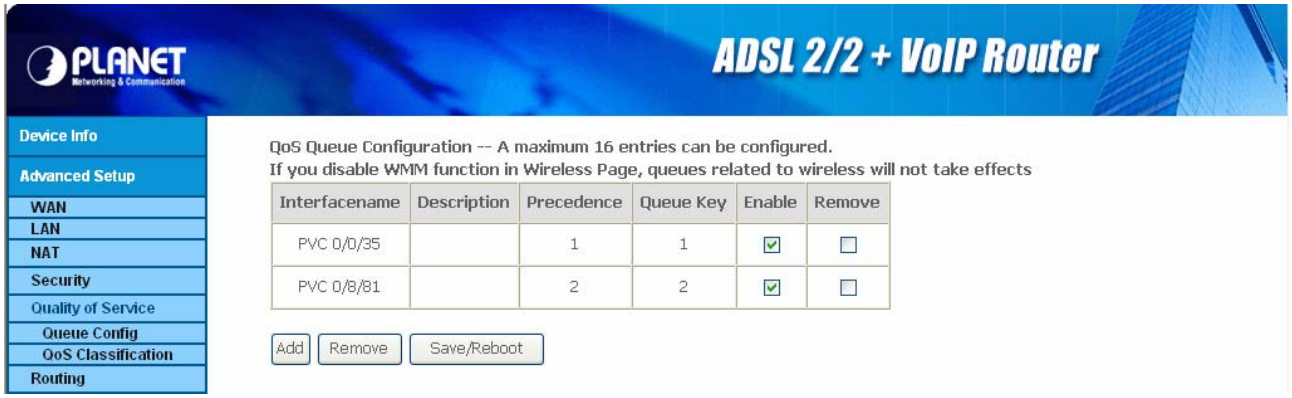


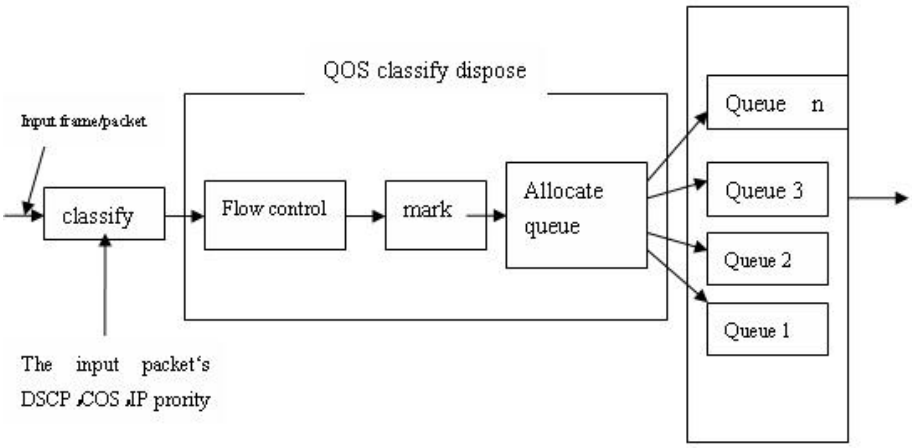
Figure: QoS Queue Config Complete

If you want to delete a certain queue, you can disable this queue and choose this queue, last click “Remove” button to delete it.

After the queue config is already configured, you can create several traffic class rules to classify the upstream traffic.

3.3.5.3 QoS -- QoS Classification

Some application require that specific bandwidths ensure its data be forward in the time. Qos classification can creates traffic class rule to classify the upstream traffic. Assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte .After Qos classification, Qos divides capacity between the different applications and provides un-delayed ,continuous data transfer where data packet with higher priority are given preference. The follow diagram show how Qos classify the



Click “Qos Classification” to pop up an interface as below. In this interface, you can configure network traffic classes.

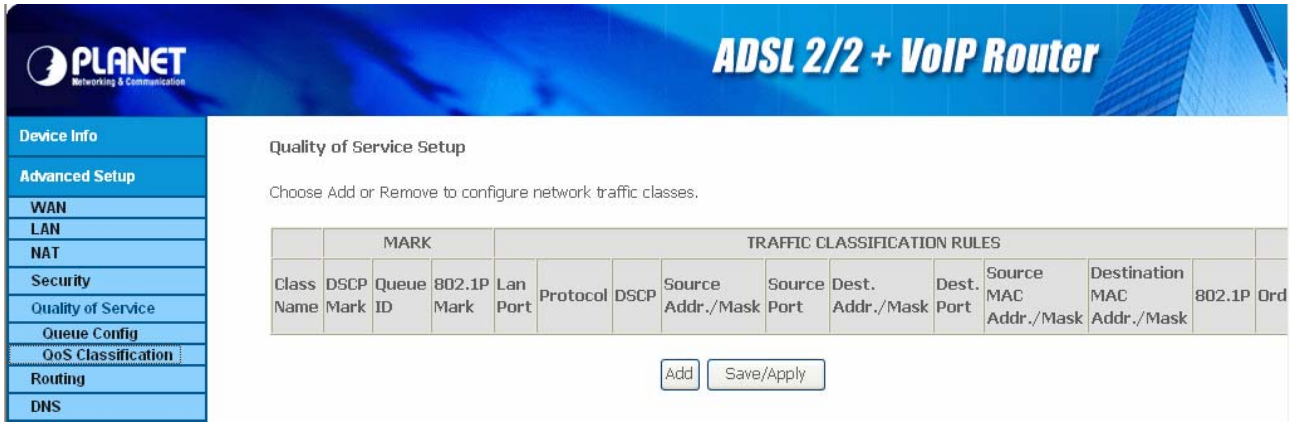


Figure: Qos Classification Conifg overview

Click “Add” to show the following interface.

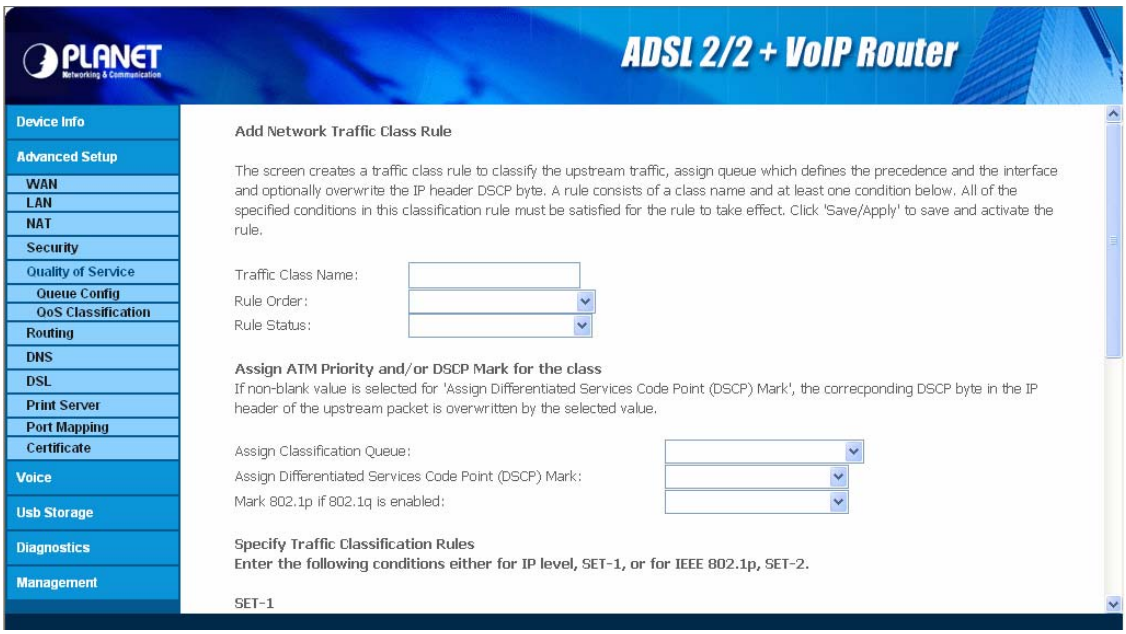

PLANET
ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Queue Config
QoS Classification
Routing
DNS
DSL
Print Server
Port Mapping
Certificate
Voice
Usb Storage
Diagnostics
Management
Add Network Traffic Class Rule
The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.
Traffic Class Name:
Rule Order:
Rule Status:
Assign ATM Priority and/or DSCP Mark for the class
If non-blank value is selected for 'Assign Differentiated Services Code Point (DSCP) Mark', the correcponding DSCP byte in the IP header of the upstream packet is overwritten by the selected value.
Assign Classification Queue:
Assign Differentiated Services Code Point (DSCP) Mark:
Mark 802.1p if 802.1q is enabled:
Specify Traffic Classification Rules
Enter the following conditions either for IP level, SET-1, or for IEEE 802.1p, SET-2.
SET-1

Figure: Qos Classification Conifg

- Traffic Class Name: Enter a name of the class
- Rule Order: Select order for queue
- Rule Status: Enable or disable this traffic class rule
- Assign Classfication Queue: Select a classification queue
- Assign Differentiated Service Code Point(DSCP)Mark: Select a mark service that will modify the original packet IP header if all the rules defined within the classification class are matched .(CS ---Mark IP Precedence AF----Assured Forwarding EF---Expedited Forwarding)
- Mark 802.1p if 802.1q is enabled: select an 802.1p priority number that will serve as the 802.1p value.

There are two sets of classification rules. Set-1 is based on different fields within TCP/UDP/IP layer plus physical LAN port; Set-2 is based on MAC layer IEEE 802.1p priority field.

Set-1 Rules contain the following

- Physical LAN port: select one among Ethernet ports
- Protocol: select one among TCP/UDP TCP UDP or ICMP protocols
- Source IP address
- Source subnet mask
- UPD/TCP source port or a range of ports
- Destination IP address
- Destination subnet mask
- UPD/TCP destination port or a range of ports
- Source Mac address
- Source Mac mask
- Destination Mac address
- Destination Mac Mask

Set-2 Rules contain the following:

- 802.1p priority: The 802.1p header includes a 3-bit prioritization field , which allows packets to be grouped into eight levels of priority(0-7), where level 7 is the highest one.

Qos -- DSCP setting

In order to understand what is Differentiated Services Code Point (DSCP), one must first be familiarized with the Differentiated Services model.

Differentiated Services (Diffserv) is a Class of Service (COS) model that enhances best-effort Internet services by differentiating traffic by users, service requirements and other criteria. Packets are specifically marked, allowing network nodes to provide different levels of service,

Via priority queuing or bandwidth allocation, or by choosing dedicated routes for specific traffic flows.

For example: Marking each transmitted ICMP packet which passing traffic to 8-81class with an appropriate DSCP (CS5). After set in the following interface:

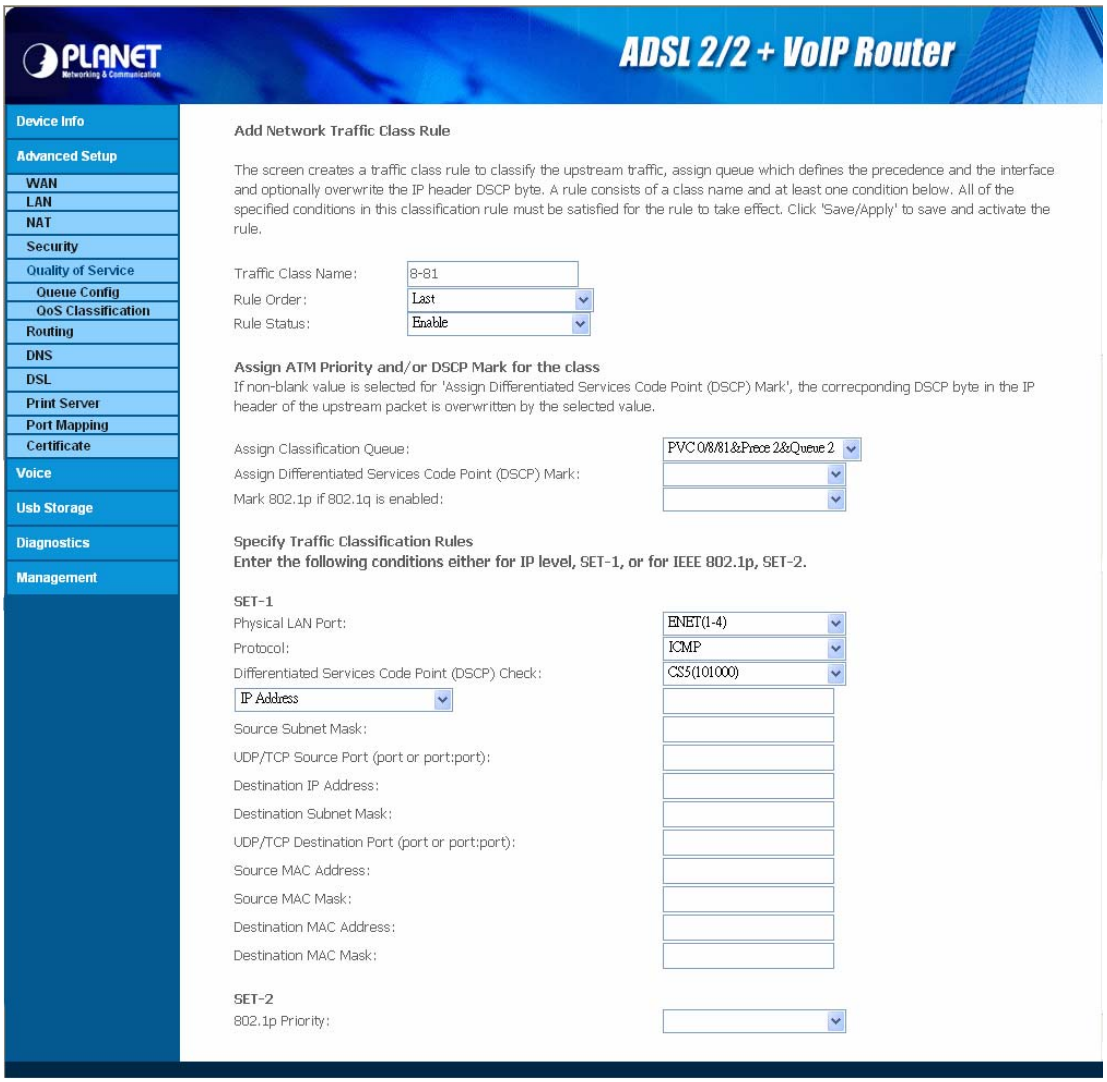

PLANET
ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Queue Config
QoS Classification
Routing
DNS
DSL
Print Server
Port Mapping
Certificate
Voice
Usb Storage
Diagnostics
Management
Add Network Traffic Class Rule
The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.
Traffic Class Name: 8-81
Rule Order: Last
Rule Status: Enable
Assign ATM Priority and/or DSCP Mark for the class
If non-blank value is selected for 'Assign Differentiated Services Code Point (DSCP) Mark', the correcponding DSCP byte in the IP header of the upstream packet is overwritten by the selected value.
Assign Classification Queue: PVC 0/8/81&Prece 2&Queue 2
Assign Differentiated Services Code Point (DSCP) Mark:
Mark 802.1p if 802.1q is enabled:
Specify Traffic Classification Rules
Enter the following conditions either for IP level, SET-1, or for IEEE 802.1p, SET-2.
SET-1
Physical LAN Port: ENET(1-4)
Protocol: ICMP
Differentiated Services Code Point (DSCP) Check: CS5(101000)
IP Address
Source Subnet Mask:
UDP/TCP Source Port (port or port:port):
Destination IP Address:
Destination Subnet Mask:
UDP/TCP Destination Port (port or port:port):
Source MAC Address:
Source MAC Mask:
Destination MAC Address:
Destination MAC Mask:
SET-2
802.1p Priority:

Figure: Qos DSCP setting Conifg example

After proper modifications, click “Save/Apply” to show the following interface.

Figure: Qos Classification Conifg Complete

Click “Save/Apply”.(This configuration will take effective at once.)

Qos -- 802.1p setting

The IEEE802.1p priority marking method is a standard for prioritizing network traffic at the data link/Mac sub-layer 802.1p traffic is simply classified and sent to the destination, with no bandwidth reservations established.

For example: Mark the frame of 802.1p that queued to Queue 1 on value 2. After set in the following interface:

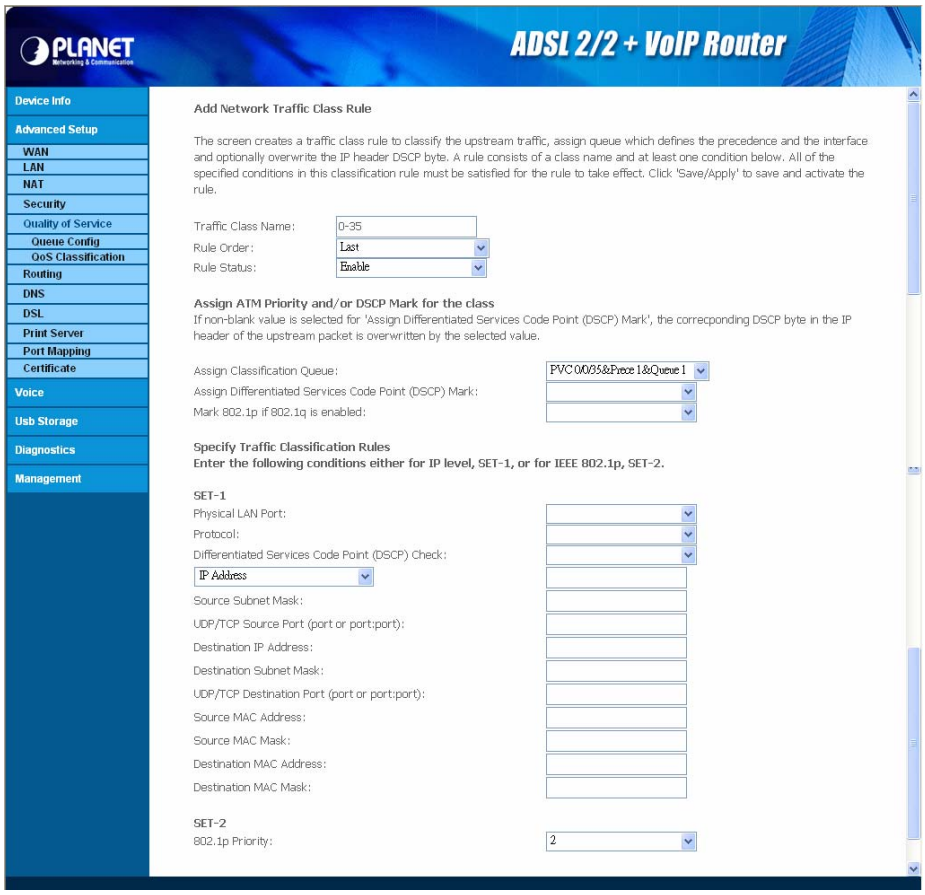

PLANET
ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Queue Config
QoS Classification
Routing
DNS
DSL
Print Server
Port Mapping
Certificate
Voice
Usb Storage
Diagnostics
Management
Add Network Traffic Class Rule
The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.
Traffic Class Name:
0-35
Rule Order:
Last
Rule Status:
Enable
Assign ATM Priority and/or DSCP Mark for the class
If non-blank value is selected for 'Assign Differentiated Services Code Point (DSCP) Mark', the correcponding DSCP byte in the IP header of the upstream packet is overwritten by the selected value.
Assign Classification Queue:
PVC 0/0/35&Prece 1&Queue 1
Assign Differentiated Services Code Point (DSCP) Mark:
Mark 802.1p if 802.1q is enabled:
Specify Traffic Classification Rules
Enter the following conditions either for IP level, SET-1, or for IEEE 802.1p, SET-2.
SET-1
Physical LAN Port:
Protocol:
Differentiated Services Code Point (DSCP) Check:
IP Address
Source Subnet Mask:
UDP/TCP Source Port (port or port:port):
Destination IP Address:
Destination Subnet Mask:
UDP/TCP Destination Port (port or port:port):
Source MAC Address:
Source MAC Mask:
Destination MAC Address:
Destination MAC Mask:
SET-2
802.1p Priority:
2

Figure: QoS 802.1p setting

After proper modifications, click “Save/Apply” to show the following interface.

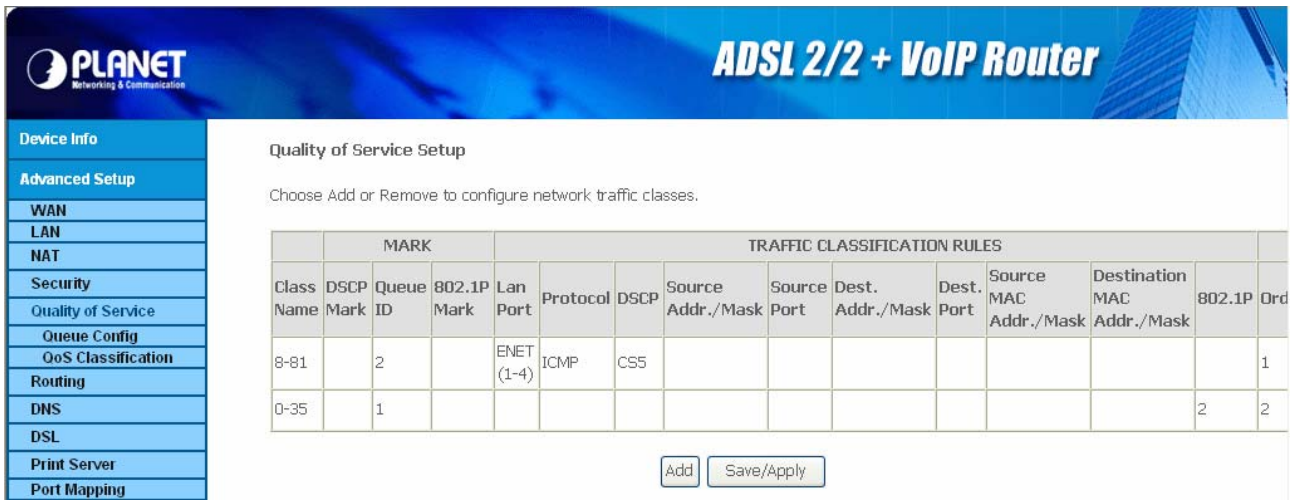


Figure: QoS 802.1p setting Complete

Click “Save/Apply”. (This configuration will take effective at once.)

3.3.6 Routing

3.3.6.1 Routing – Default Gateway

In this interface, you can modify the Default Gateway settings.

If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.

> **NOTE:**
> If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.

- If you want to use a default gateway, please click “ENABLE Automatic Assigned Default Gateway” box to show the following interface.

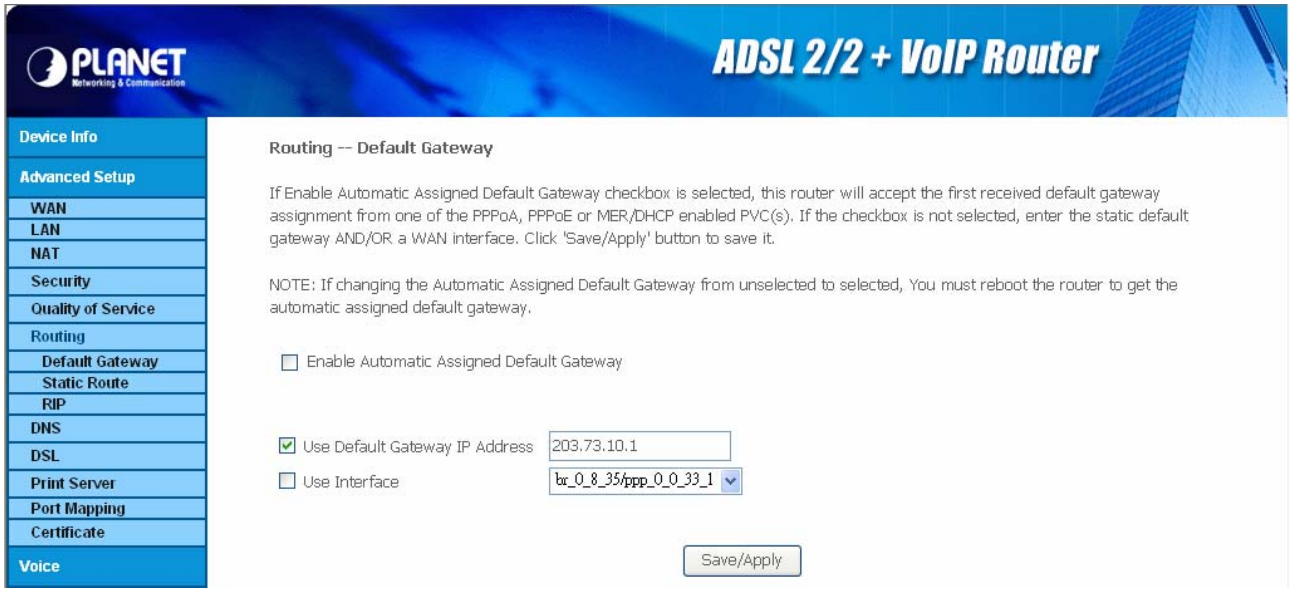

PLANET
Networking & Communication
ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
Default Gateway
Static Route
RIP
DNS
DSL
Print Server
Port Mapping
Certificate
Voice
Routing -- Default Gateway
If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.
NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.
Enable Automatic Assigned Default Gateway
Use Default Gateway IP Address
203.73.10.1
Use Interface
br_0_8_35/ppp_0_0_33_1
Save/Apply

Figure: Default Gateway

Use Default Gateway

- Select “Enable automatic Assigned Default Gateway” box

Custom DSL router Default Gateway

- Close “Enable automatic Assigned Default Gateway” box
- Entry Use Default Gateway IP Address
- Entry Use Interface: The interface that the packets pass through on the ROUTER.
- Apply setting by click Save/Apply

3.3.6.2 Static Routes

Networking devices forward packets using route information that is either manually configured or dynamically learned using a routing protocol. Static routes are manually configured and define an explicit path between two networking devices. Unlike a dynamic routing protocol, static routes are not automatically updated and must be manually reconfigured if the network topology changes. The benefits of using static routes include security and resource efficiency. Static routes use less bandwidth than dynamic routing protocols and no CPU cycles are used to calculate and communicate routes. The main disadvantage to using static routes is the lack of automatic reconfiguration if the network topology changes.

Static routes can be redistributed into dynamic routing protocols but routes generated by dynamic routing protocols cannot be redistributed into the static routing table. No algorithm exists to prevent the configuration of routing loops that use static routes.

Static routes are useful for smaller networks with only one path to an outside network and to provide security for a larger network for certain types of traffic or links to other networks that need more control. In general, most networks use dynamic routing protocols to communicate between networking devices but may have one or two static routes configured for special cases

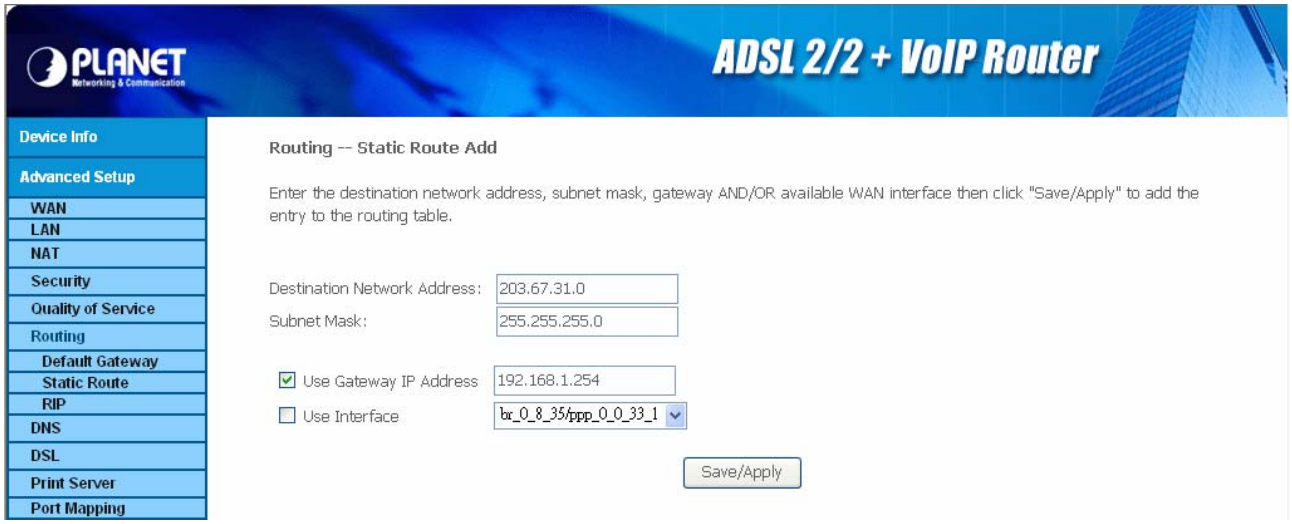


Figure: Static routes Add Config

Add static route

- Entry destination network address
- Entry subnet Mask
- Enable “Use Gateway IP Address” and entry IP address
- Select use interface
- Apply setting by click Save/Apply

Remove static route

- Select “remove” box on table
- Apply setting by click “remove”

3.3.6.3 RIP

Background

The Routing Information Protocol, or RIP, as it is more commonly called, is one of the most enduring of all routing protocols. RIP is also one of the more easily confused protocols because a variety of RIP-like routing protocols proliferated, some of which even used the same name! RIP and the myriad RIP-like protocols were based on the same set of algorithms that use distance vectors to mathematically compare routes to identify the best path to any given destination address. These algorithms emerged from academic research that dates back to 1957. Today's open standard version of RIP, sometimes referred to as IP RIP, is formally defined in two documents: Request For Comments (RFC) 1058 and Internet Standard (STD) 56. As IP-based networks became both more numerous and greater in size, it became apparent to the Internet Engineering Task Force (IETF) that RIP needed to be updated. Consequently, the IETF released RFC 1388 in January 1993, which was then superseded in November 1994 by RFC 1723, which describes RIP 2 (the second version of RIP). These RFCs described an extension of RIP's capabilities but did not attempt to obsolete the previous version of RIP. RIP 2 enabled RIP messages to carry more information, which permitted the use of a simple authentication mechanism to secure table updates. More importantly, RIP 2 supported subnet masks, a critical feature that was not available in RIP.

This chapter summarizes the basic capabilities and features associated with RIP. Topics include the routing update process, RIP routing metrics, routing stability, and routing timers.

Routing Updates

RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop. RIP routers maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change. These updates are sent independently of the regularly scheduled updates that RIP routers send

RIP Routing Metric

RIP uses a single routing metric (hop count) to measure the distance between the source and a destination network. Each hop in a path from source to destination is assigned a hop count value, which is typically 1. When a router receives a routing update that contains a new or changed destination network entry, the router adds 1 to the metric value indicated in the update and enters the network in the routing table. The IP address of the sender is used as the next hop

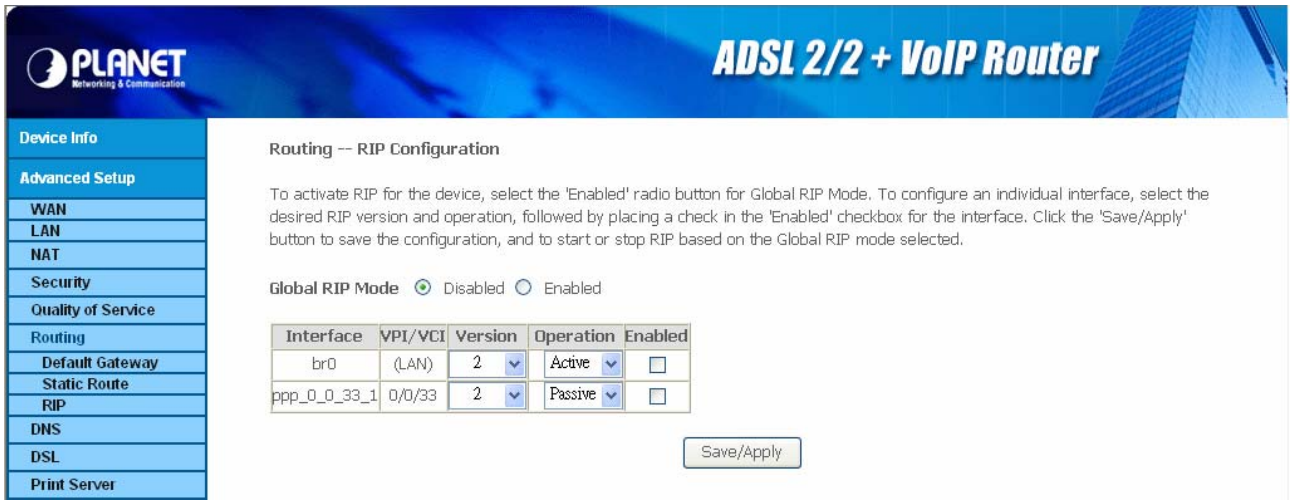

PLANET
Networking & Communication
ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
Default Gateway
Static Route
RIP
DNS
DSL
Print Server
Routing -- RIP Configuration
To activate RIP for the device, select the 'Enabled' radio button for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the 'Enabled' checkbox for the interface. Click the 'Save/Apply' button to save the configuration, and to start or stop RIP based on the Global RIP mode selected.
Global RIP Mode Disabled Enabled
Interface VPI/VCI Version Operation Enabled
br0 (LAN) 2 Active
ppp_0_0_33_1 0/0/33 2 Passive
Save/Apply

Figure: RIP Configuration

RIP configuration

- To activate RIP for the device, select the 'Enabled' radio button for Global RIP Mode.
- To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the 'Enabled' checkbox for the interface.

Click the 'Save/Apply' button to save the configuration, and to start or stop RIP based on the Global RIP mode selected.

3.3.7 DNS

Short for **D**omain **N**ame **S**ystem (or **S**ervice or **S**erver), an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4.

The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

3.3.7.1 DNS Server

In this interface, you can modify the DNS server settings.

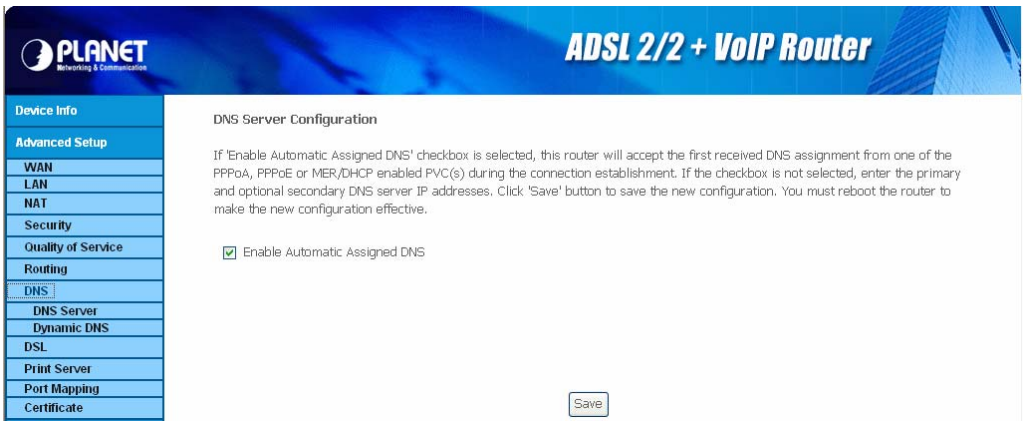

PLANET
ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
DNS
DNS Server
Dynamic DNS
DSL
Print Server
Port Mapping
Certificate
DNS Server Configuration
If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the router to make the new configuration effective.
Enable Automatic Assigned DNS
Save

Figure: DNS Server Configuration overview

If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment.

If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. The interface is below.

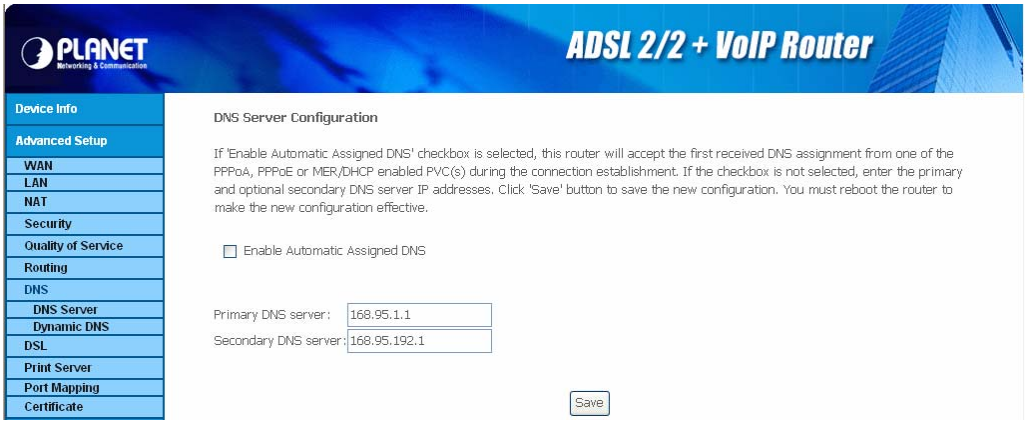

PLANET
ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Quality of Service
Routing
DNS
DNS Server
Dynamic DNS
DSL
Print Server
Port Mapping
Certificate
DNS Server Configuration
If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the router to make the new configuration effective.
Enable Automatic Assigned DNS
Primary DNS server: 168.95.1.1
Secondary DNS server: 168.95.192.1
Save

Figure: DNS Server Add Configuration

Click 'Save' button to save the new configuration.

NOTE: You must reboot the router to make the new configuration effective.

3.3.7.2 Dynamic DOMAIN NAME SERVICE (DDNS)

OVERVIEW

Dynamic DNS allows binding of domain names to hosts with dynamically assigned IP addresses by a Dynamic Host Control Protocol (DHCP) server and updates the name server with the new information about the host or the network. This is particularly useful to broadband users hosting internet services such as File Transfer Protocol (FTP), Hyper Text Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP) on their local hosts connected to the broadband network at home. Dynamic DNS allows access to such hosts connected to the broadband networks using a domain name to exchange files, send receive email with highly personalized email addresses and host a website. The primary requirement in such case is for the domain name to be associated with the ever changing IP address of the host or the network. For more details about dynamic DNS please refer to RFC 2136.

To provide such support for the feature described above, a client is installed in the host serving the internet traffic directed to the domain. The client updates the IP address of the host whenever the host renegotiates the IP address for any reason. The system provides support for dynamic DNS allows the users to configure the following dynamic DNS servers for DDNS service:

- **DynDNS.org**: A free DNS service for hosts with dynamic IP addresses.
- **TZO**: A service provider providing dynamic and static DNS services for a fee.

To use one of the providers mentioned above requires the users to register with the dynamic DNS service provider the information about the host and the install the client software on the host which can update the service provider with the IP address and the domain name information.

CONFIGURATION

The DDNS feature in Linux reference software requires to be configured in the menu config to include the support for this feature. Once the software support is configured to be built for a profile, this feature can be configured using the WEB UI as:

- Choose the Advanced Setup from the WEB UI, choose the DNS menu item under Advanced
- Setup and select the Dynamic DNS menu item under DNS.

Figure: Dynamic DNS Configuration overview

- Click the Add button to configure new host information.

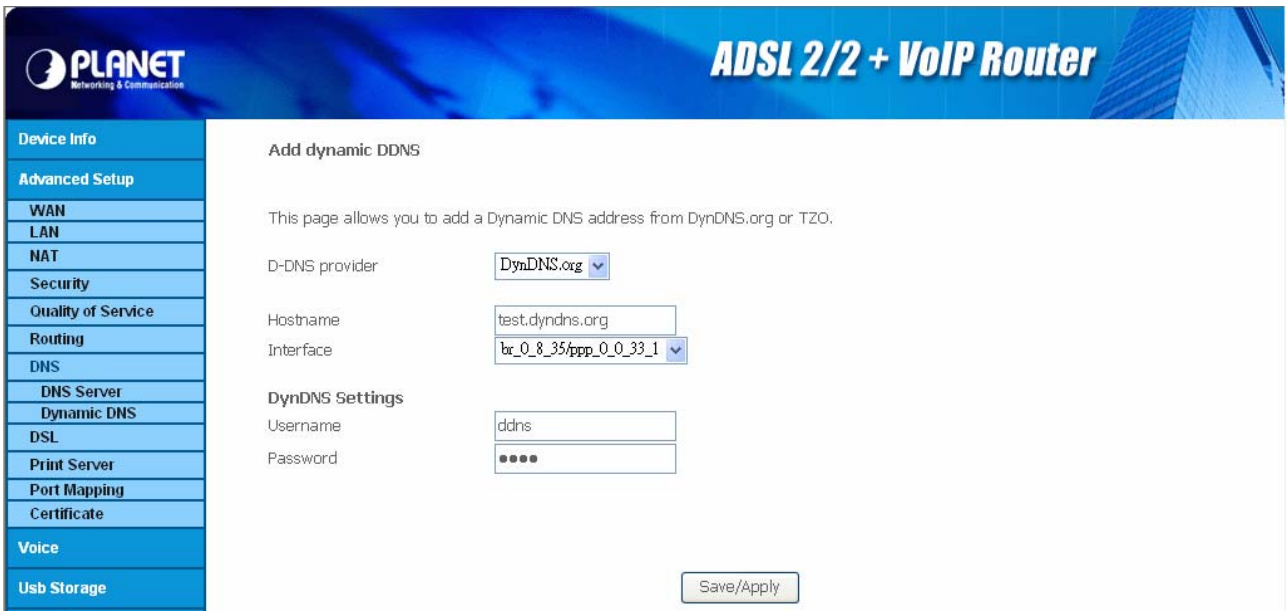


Figure: Dynamic DNS Add Configuration

- **D-DNS provider:** Dynamic DNS provider's website.
- **Hostname:** This is the domain name which can be modified.
- **Interface**: The interface that the packets pass through on the ROUTER.
- **Username:** This is the Username needed access the DDNS's management interface.
- **Password:** This is the Password you will be prompted to enter when you access the DDNS's management interface.

➢ Select the service provider for the DDNS service; provide the hostname and the interface to use when sending the DDNS updates. Also enter the service provider specific registration information and click Save/Apply to use the feature.

3.3.8 DSL

In this interface, you can check the DSL settings. Mostly, the user just need to remain this factory default setting. Our Router support these modulations: G.Dmt, G.lite, T1.413, ADSL2, AnnexL, ADSL2+ and AnnexM. The ROUTER will negotiate the modulation mode with the DSLAM.

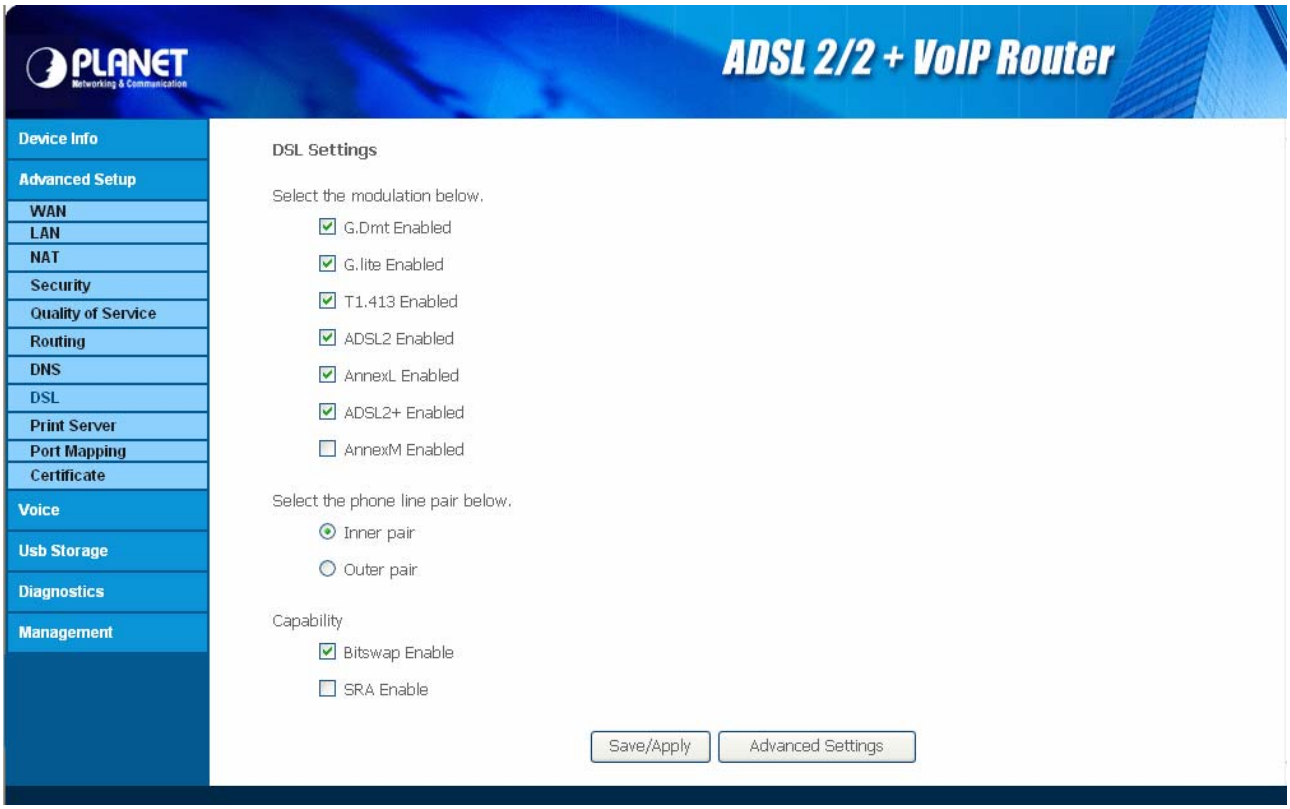


Figure: DSL modulation settings

3.3.9 Print Server

A network printer is a printer on which you can print your documents without it being connected to your pc. The advantage of this is that you only need this printer once in your network. All PCs for which it is released can access it and work with it.

In most cases a printer of this type is connected to another PC in the network. This does indeed offer the advantage referred to above, but it has serious disadvantages:

- The printer can only be used by others if the PC to which it is connected is switched on.
- The print job you send to the PC on which the printer depends reduces the performance of this PC.

To facilitate this option you must first set up a printer port on each PC that is to use the network printer. A printer port is an interface on the PC that forwards the print job to an IP address within the network. Once you have set up this port you must install the printer driver.

3.3.9.1 Configuring Print Server on DSL Server

Following are the steps to enable the on-board Printer Server for HP-3845.

Step 1. Enable Print Server from Router Web GUI.

Step 2. Check “Enable on-board printer server” and key in “Printer name”, “Make and model”. This example please type “**hp3845**” as Printer name.

Note:

The “Printer name” can be any text string up to **40** characters.

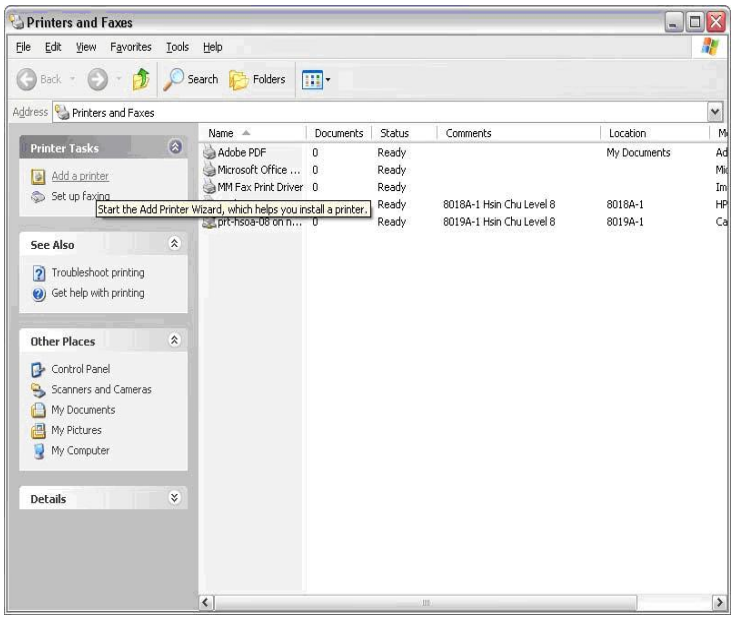
The “Make and model” can be any text string up to **128** characters.

Figure: Print Server Config

3.3.9.2 Configuring Print Server on the Windows Host

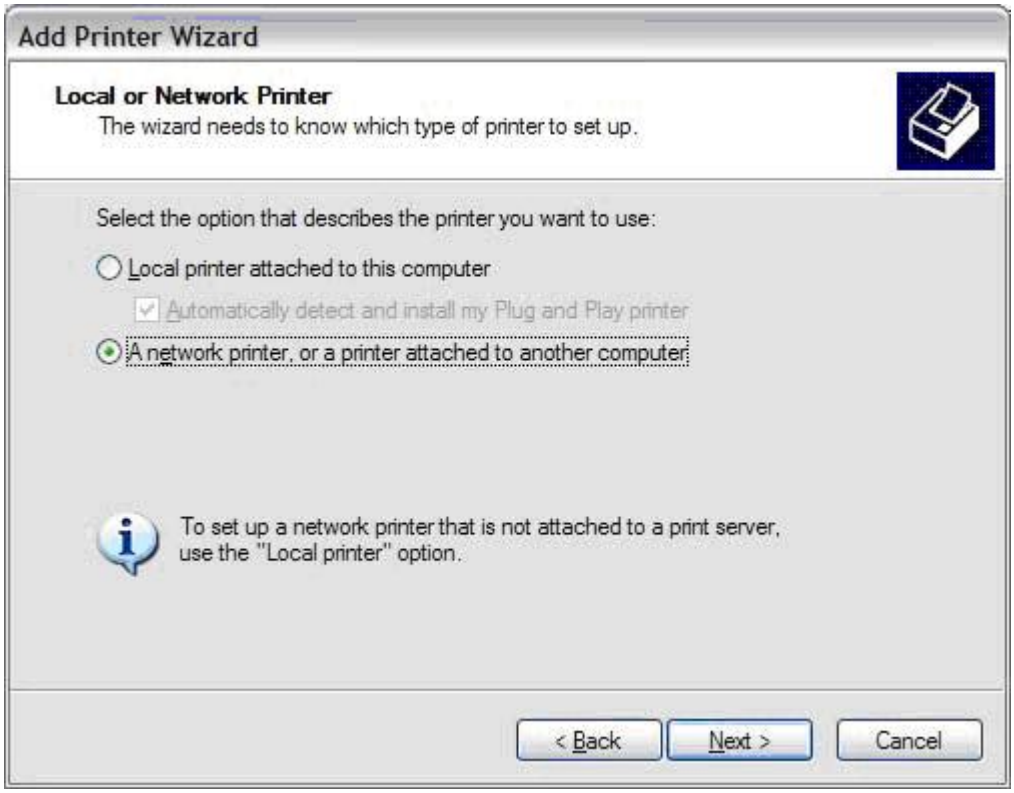
The configuring sequence:

Step 1. Click on Add a printer from **Control Panel** of the **Win XP** computer and click "Next".



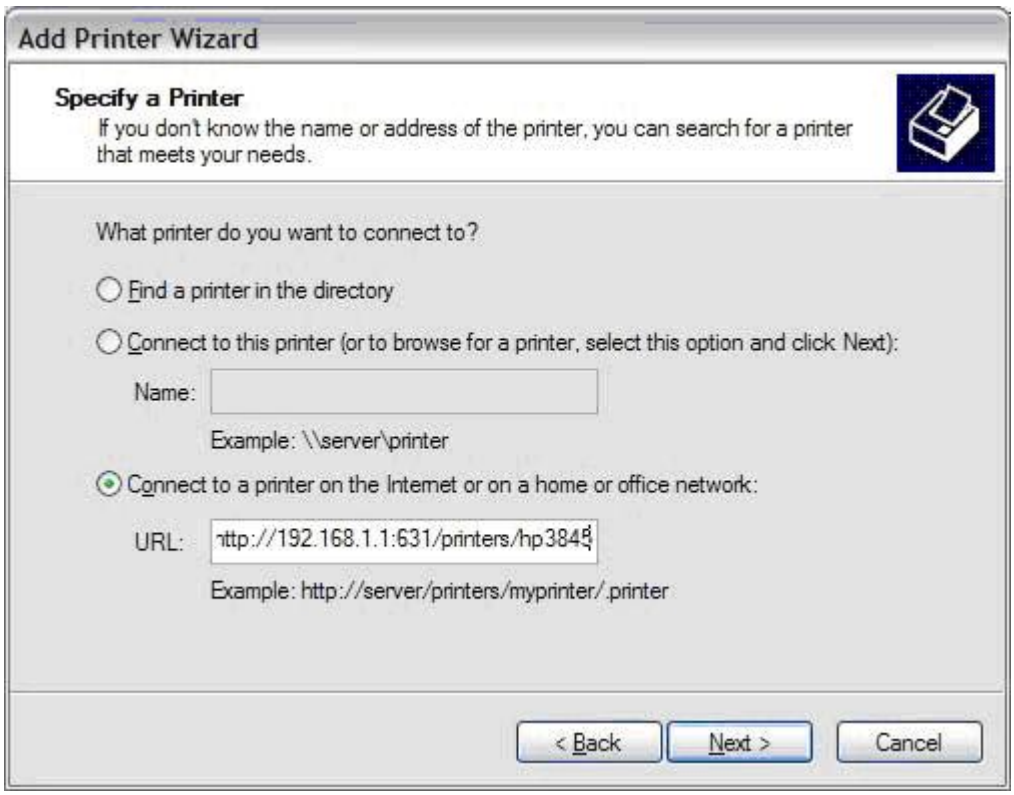
Add Printer Wizard
Welcome to the Add Printer Wizard
This wizard helps you install a printer or make printer connections.
If you have a Plug and Play printer that connects through a USB port (or any other hot pluggable port, such as IEEE 1394, infrared, and so on), you do not need to use this wizard. Click Cancel to close the wizard, and then plug the printer's cable into your computer or point the printer toward your computer's infrared port, and turn the printer on. Windows will automatically install the printer for you.
To continue, click Next.
< Back
Next >
Cancel

Step 2. Select Network Printer and click “Next”.


Add Printer Wizard
Local or Network Printer
The wizard needs to know which type of printer to set up.
Select the option that describes the printer you want to use:
Local printer attached to this computer
Automatically detect and install my Plug and Play printer
A network printer, or a printer attached to another computer
To set up a network printer that is not attached to a print server, use the "Local printer" option.
< Back
Next >
Cancel

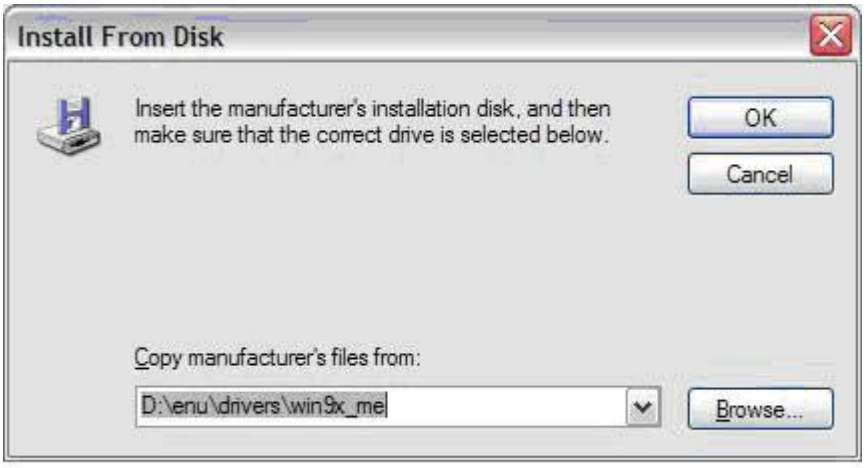
Step 3. Select Connect to a printer on the Internet, type “**http://192.168.1.1:631/printers/hp3845**” and click “Next”.

The printer name “hp3845” must be the same name entered in the ADSL Router WEB UI “printer server setting” as before.


Add Printer Wizard
Specify a Printer
If you don't know the name or address of the printer, you can search for a printer that meets your needs.
What printer do you want to connect to?
Find a printer in the directory
Connect to this printer (or to browse for a printer, select this option and click Next):
Name:
Example: \\server\printer
Connect to a printer on the Internet or on a home or office network:
URL:
http://192.168.1.1:631/printers/hp3845
Example: http://server/printers/myprinter/.printer
< Back
Next >
Cancel

Step 4. Click “Have Disk”, insert printer driver CD.

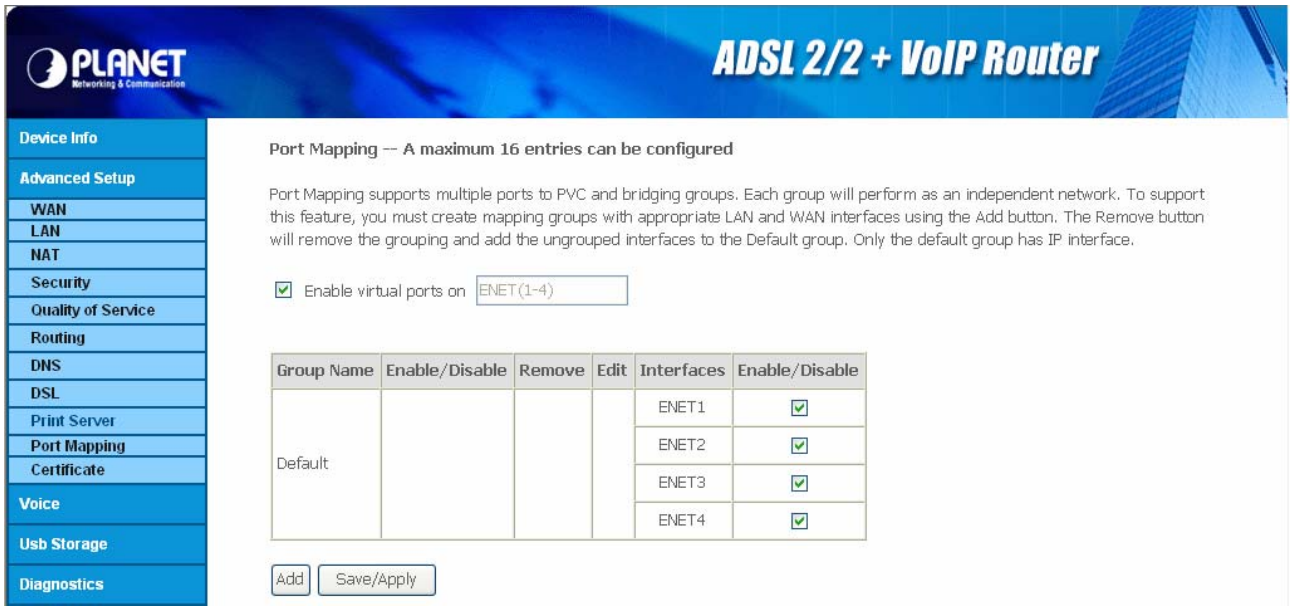
Step 5. Select driver file directory on CD-ROM and click “OK”.



3.3.10 Port Mapping

Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Selecting the “Enable virtual ports” button in WEB UI “Port Mapping” page will create three virtual interfaces within the system. Each virtual interface represents a physical Ethernet port within the external Ethernet Switch. The WEB UI will display four Ethernet ports: ENET1, ENET2, ENET3, and ENET4. ENET1, ENET2, and ENET3 represent Ethernet port ID 0, 1 and 2 within the Ethernet Switch. ENET4 represents the Ethernet MAC/PHY MDI port.



De-selecting the “Enable virtual ports” button will disable the system capability to recognize individual Ethernet port within the Ethernet switch.

3.3.10.1 Create a new mapping group

Group Name: Enter a unique group name.

Grouped Interfaces: The port belongs to this group.

Available Interfaces: It shows the available Ethernet port which you can select.

Automatically Add Clients With the following DHCP Vendor IDs: If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the Router to allow it to obtain an appropriate IP address. (for example, the windows 2000/XP default DHCP client's vender ID is MSFT 5.0.).

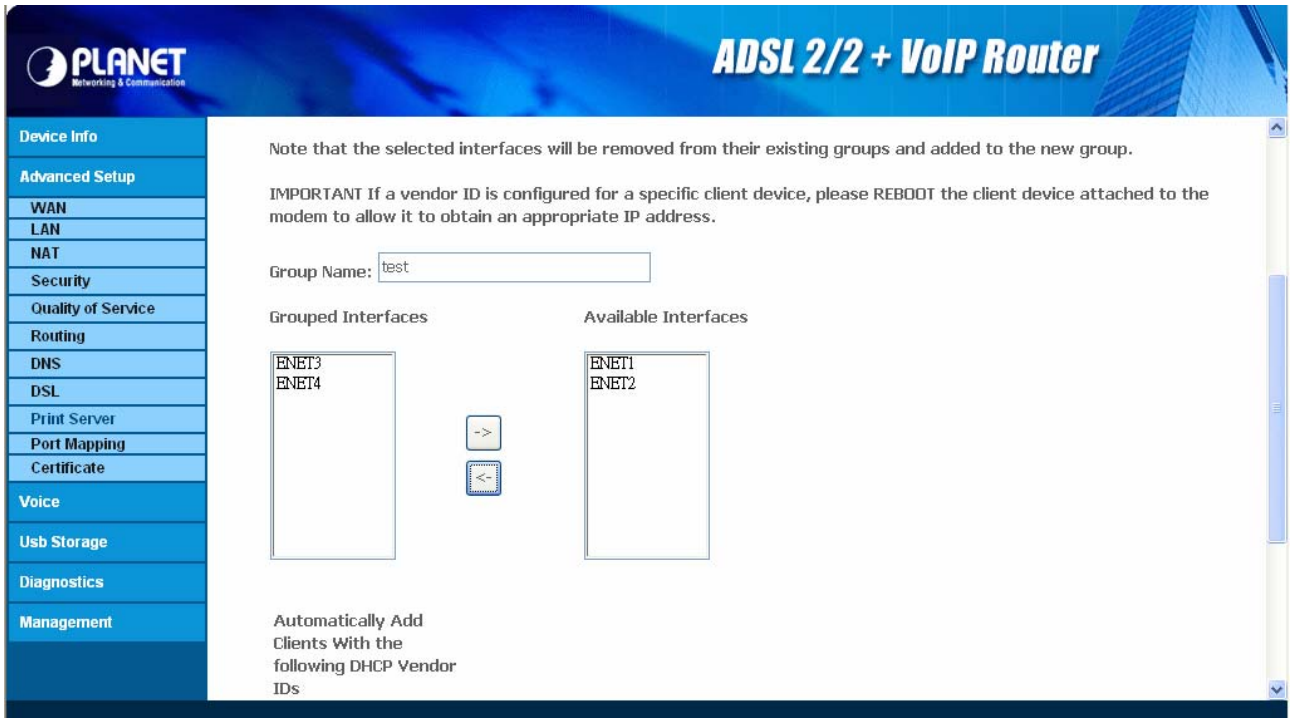


Figure: Port Mapping configuration

Step 1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.

Step 2. If you like to automatically add LAN clients to a PVC in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server. Note that these clients may obtain public IP addresses.

Step 3. Click Save/Apply button to make the changes effective immediately

Note: That the selected interfaces will be removed from their existing groups and added to the new group.

3.3.10.2 Edit a existing group

Group Name: Enter a unique group name.

Grouped Interfaces: The port belongs to this group.

Available Interfaces: It shows the available Ethernet port which you can select.

Automatically Add Clients With the following DHCP Vendor IDs: If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the Router to allow it to obtain an appropriate IP address. (For example, the windows 2000/XP default DHCP client's vender ID is MSFT 5.0.)

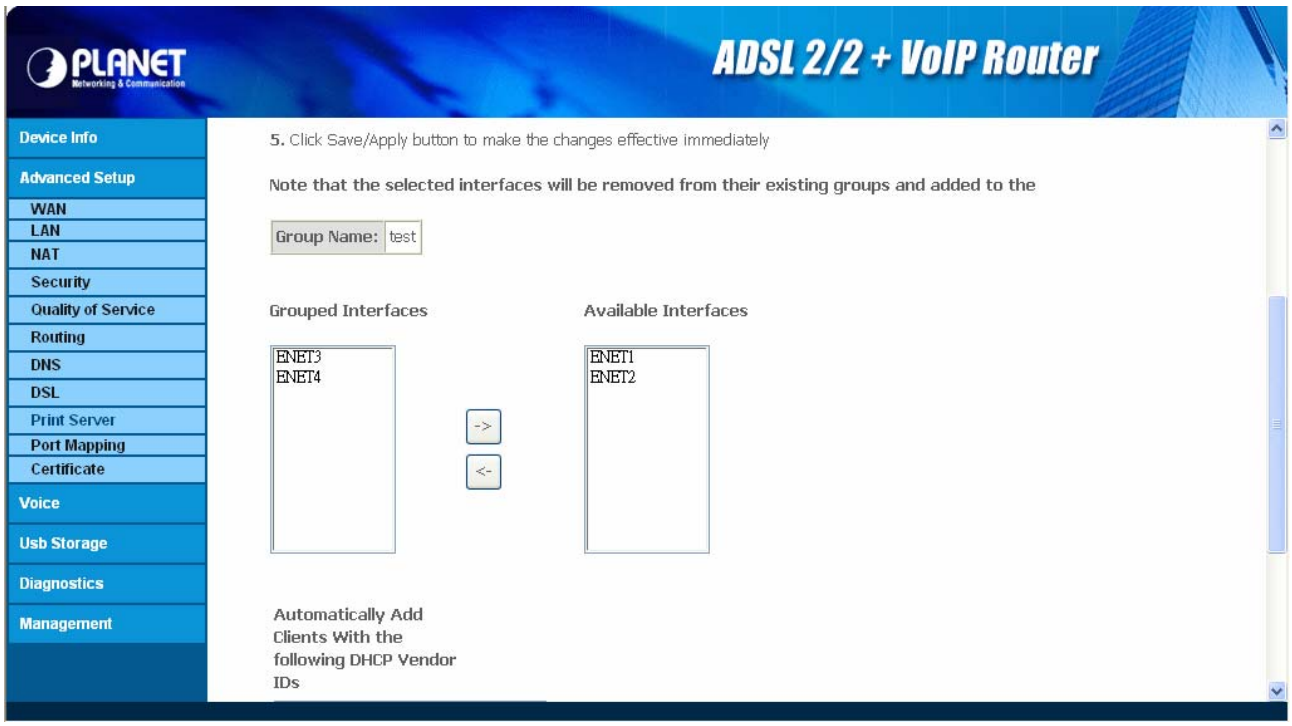


Figure: Edit Port Mapping Configuration

Edit Port Mapping Configuration

Step 1. To add interfaces to the grouped list, select the interfaces from available interface list.

Step 2. Use the left arrow button to move the selected interfaces to the grouped list.

Step 3. To remove the interfaces, select the interface from the grouped list and click the right arrow button.

Step 4. To automatically add LAN clients to the specified group PVC edit the list.

Step 5. Click Save/Apply button to make the changes effective immediately

Note: That by adding the DHCP vendor ID (OPTION 60) string. The clients will be automatically denied an IP address by the local DHCP server and may obtain public IP address.

3.3.11 Certificate

To use Certificate user interface, choose “Certificate” under “Advanced Setup” menu. There are two menu items under “Certificate” menu: “Local” and “CA”. For either type of certificate, the base screen shows a list of certificates stored in Router.

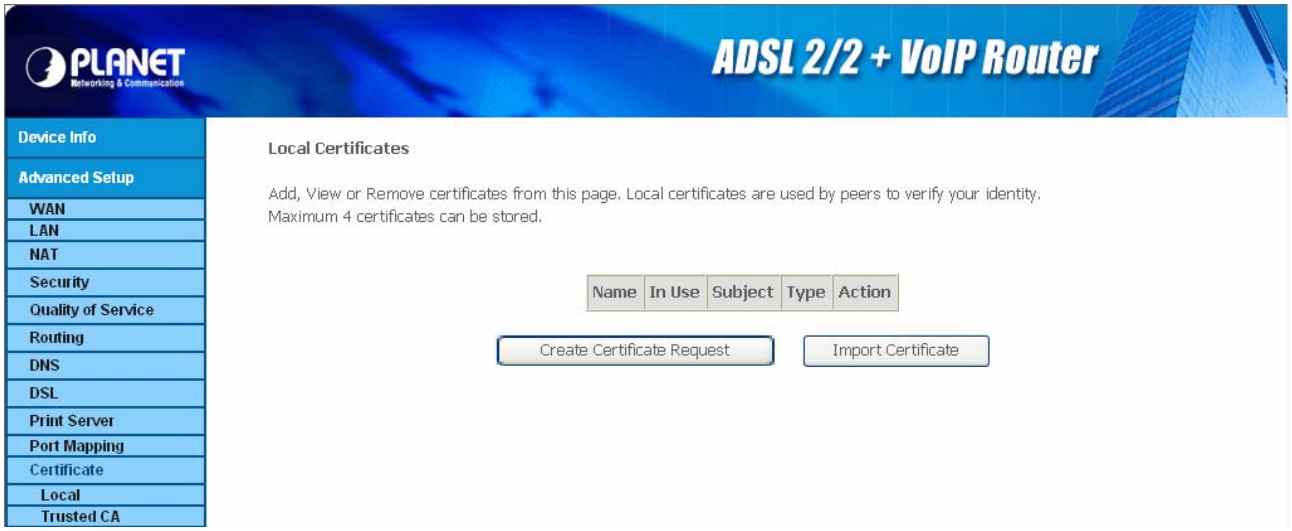


Figure: Local Certificate overview

In the menu, “Local” means local certificates. “Trusted CA” means trusted Certificate Authority certificates. Local certificates preserve the identity of the Router. CA certificates are used by the Router to very certificates from other hosts.

Local certificates can be created by two ways:

- Create a new certificate request, have it signed by a certificate authority and load the signed certificate
- Import an existing signed certificate directly

3.3.11.1 Create New Local Certificate

Certificate name:

Creates an SSL certificate in the specified certificate repository (administrator's or domain's repository) by using a private key file and a corresponding certificate file.

Common Name:

The common name is the "fully qualified domain name," (or FQDN) used for DNS lookups of your server (for example, www.mydomain.com). Browsers use this information to identify your Web site. Some browsers will refuse to establish a secure connection with your site if the server name does not match the common name in the certificate. Please do not include the protocol specify "http://" or any port numbers or pathnames in the common name. Do not use wildcard characters such as * or ? and do not use an IP address.

Organization Name:

The name of the organization to which the entity belongs (such as the name of a company).

State/Province Name:

This is the name of the state or province where your organization's head office is located. Please enter the full name of the state or province.

Country/Region Name:

This is the two-letter ISO abbreviation for your country (for example, GB for the United Kingdom).

Follow the following steps to create a new certificate:

Click “Create Certificate Request”, enter necessary information:

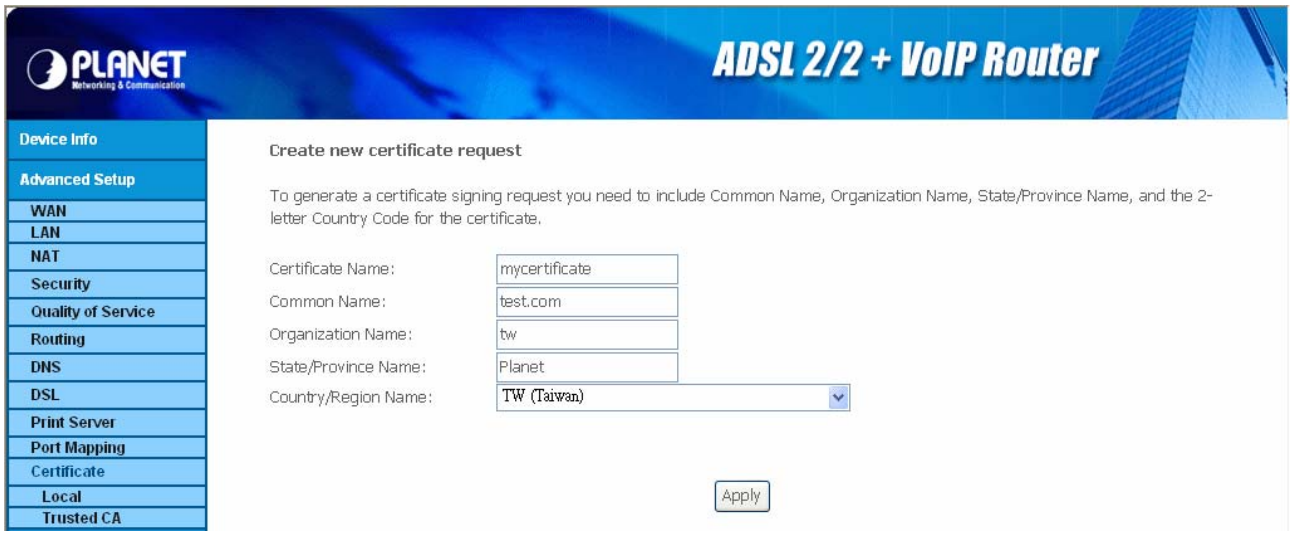


Figure: create new certificate request

Click “Apply” and wait several seconds, the generated certificate request will be shown:

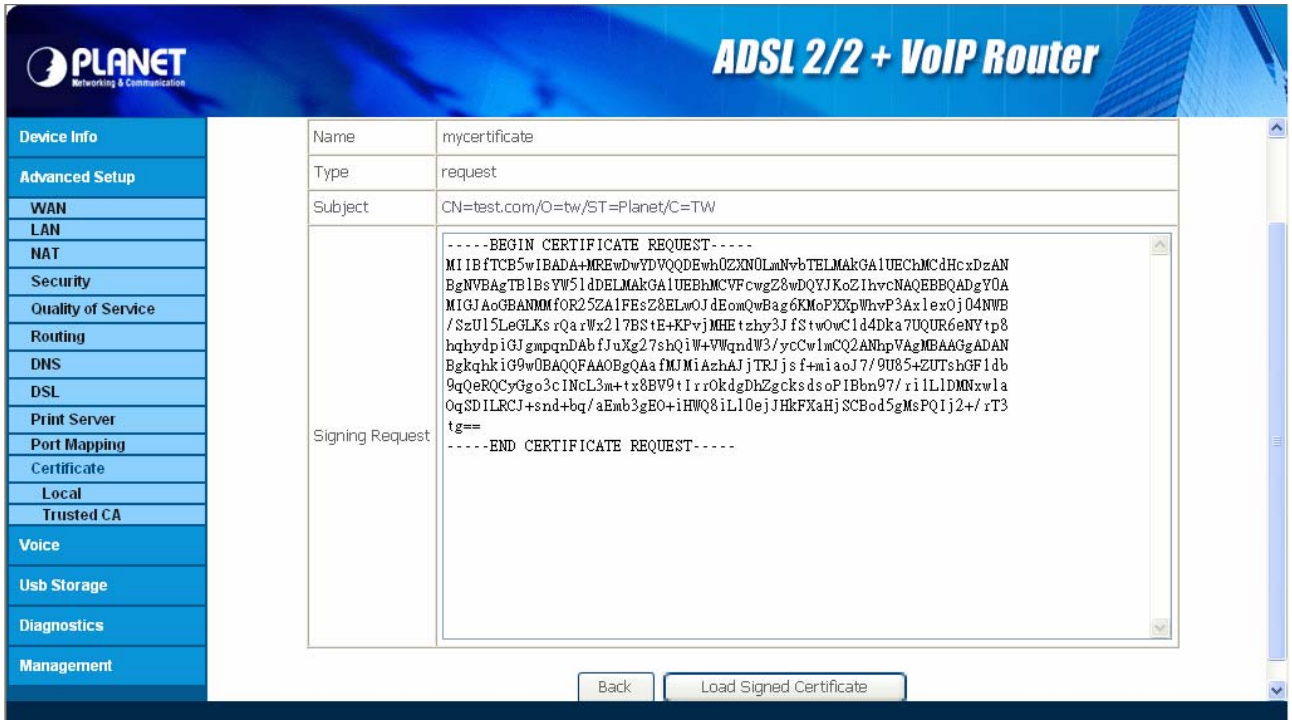


Figure: generated certificate request

The certificate request needs to be submitted to a certificate authority, which would sign the request. Then the signed certificate needs to be loaded into Router. Click “Load Certificate” button from the previous screen or from the base screen will bring up the load certificate page. Paste the signed certificate and click apply and a new certificate is created.

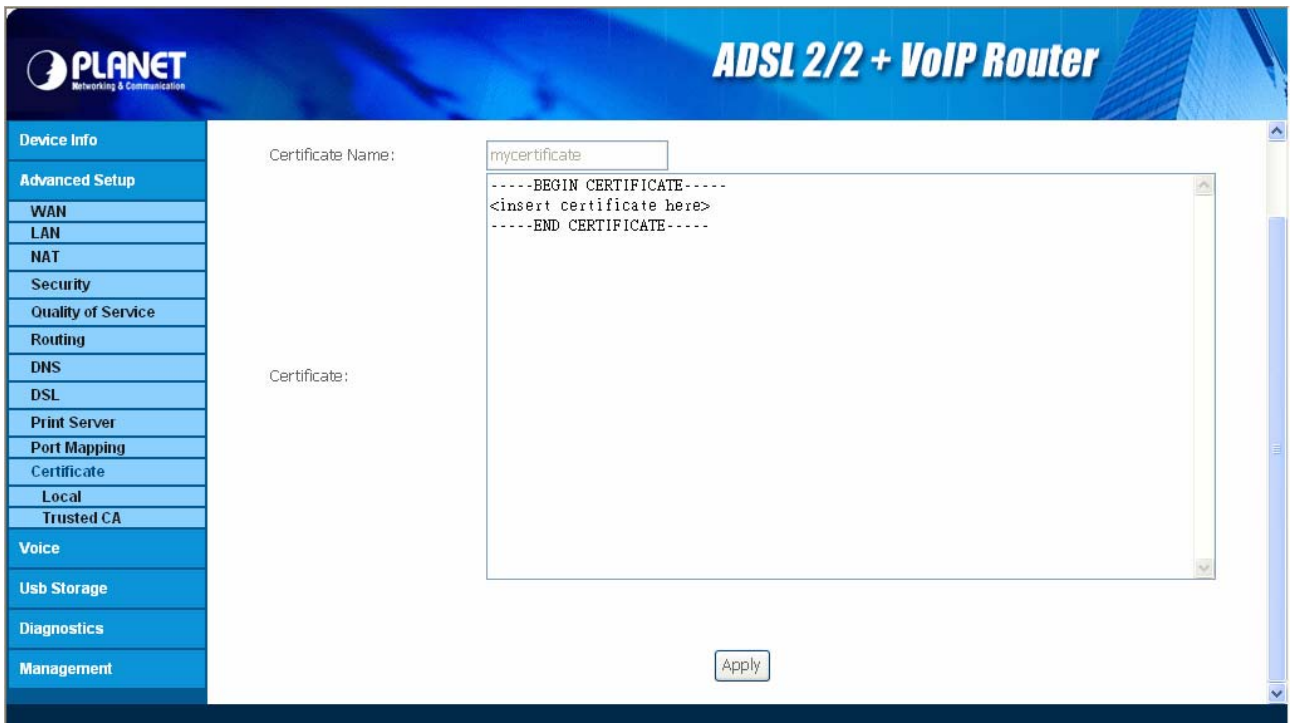


Figure: Load Certificate

3.3.11.2 Import Existing Local Certificate

To import existing certificate, click “Import Certificate” button and paste both certificate and corresponding private key:

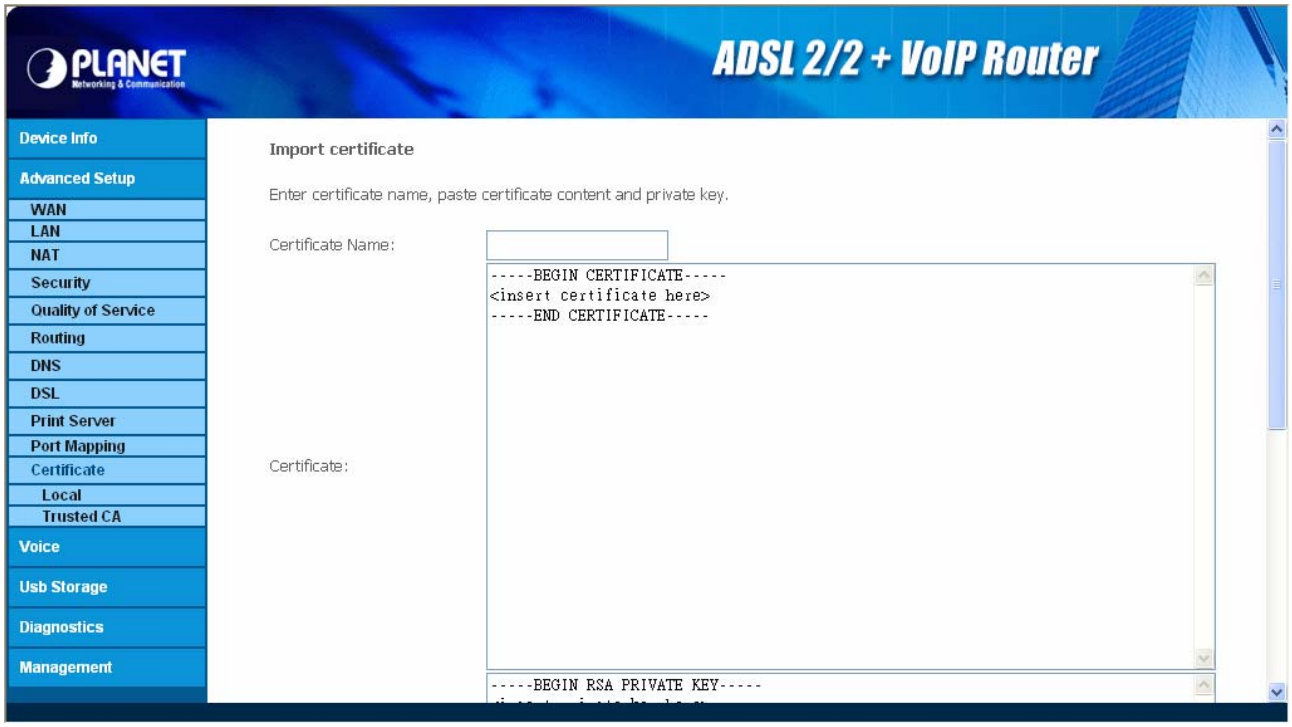


Figure: Import Certificate

3.3.11.3 Trusted CA Certificates

Click “Certificate” --> “Trusted CA” to show the interface. CA certificates are used by you to verify peers' certificates. Maximum 4 certificates can be stored.

Figure: Trusted CA certificates

Click “Import Certificate”. CA certificate can only be imported. The screen for importing is shown below:

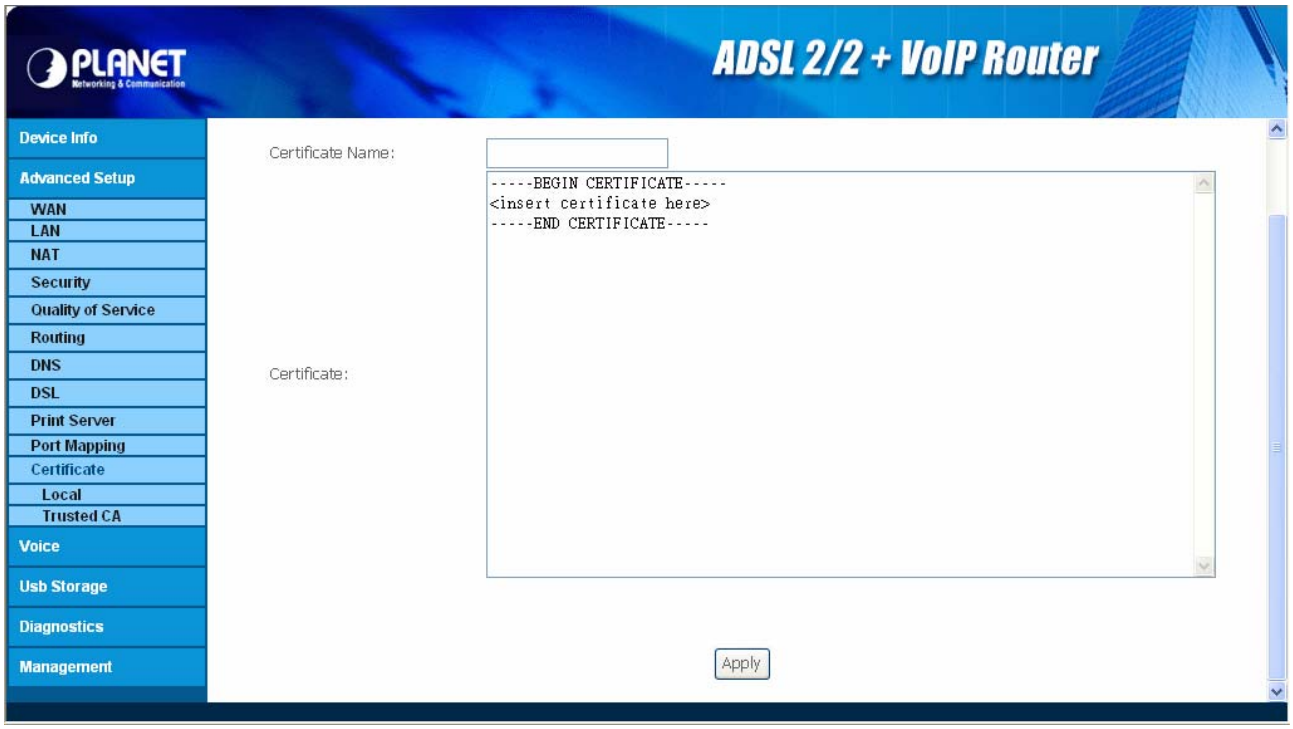


Figure: Import CA Certificate

3.4 Voice

Overview

DSL Router's Voice over IP (VoIP) solution allows you to connect two or more parties over a single broadband connection, providing the benefits and quality of digital voice and other advanced features. These parties include IP phone, analog phone attached an ATA (Analog Telephone Adapter), and telephone on PSTN network. With a PBX (Private Branch Exchange) or a signaling gateway, you can even connect to VoIP phones armed with other protocols than SIP. DSL ROUTER enables you to place and receive calls over the Internet using a standard telephone set connected to SIP Proxy or other devices which have/include the same functions as SIP Proxy.

With proper dial-plan setting, calls on DSL ROUTER may be routed to PSTN network or VoIP network, depending on what digits you dial.

DSL ROUTER provides 2 FXS interfaces and 1 FXO interface. FXO is connected to telephone line, through which you dial up to Internet. Normally the telephone line is multiplexed with both telephone signal and data signal. If not filtered out by a splitter before entering FXO interface, the incoming PSTN calls will be routed to FXS-connected analog phone or other VoIP user. You can use up to 2 analog phones, each connected to one FXS interface. The two are called endpoint, and act as a independent role as IP phones. To configure VoIP account for each endpoint, please refer to 'SIP Basic Setting' page.

Web Page Introduction

Once you have logged in web page, navigate to VoIP page from left menu tree. Here you can set some parameters you need to register SIP endpoints, place a call or some advanced feature. The VoIP page doesn't contains a 'Save' or 'Apply' button, but you can save your settings permanently by clicking '**Stop SIP client**' or '**Start SIP client**'.

3.4.1 SIP Basic Setting

Access the SIP Basic setting by clicking the ‘SIP Basic Setting’ tab under the ‘Voice’ menu. The SIP Basic Setting screen appears, it shows as below figure.

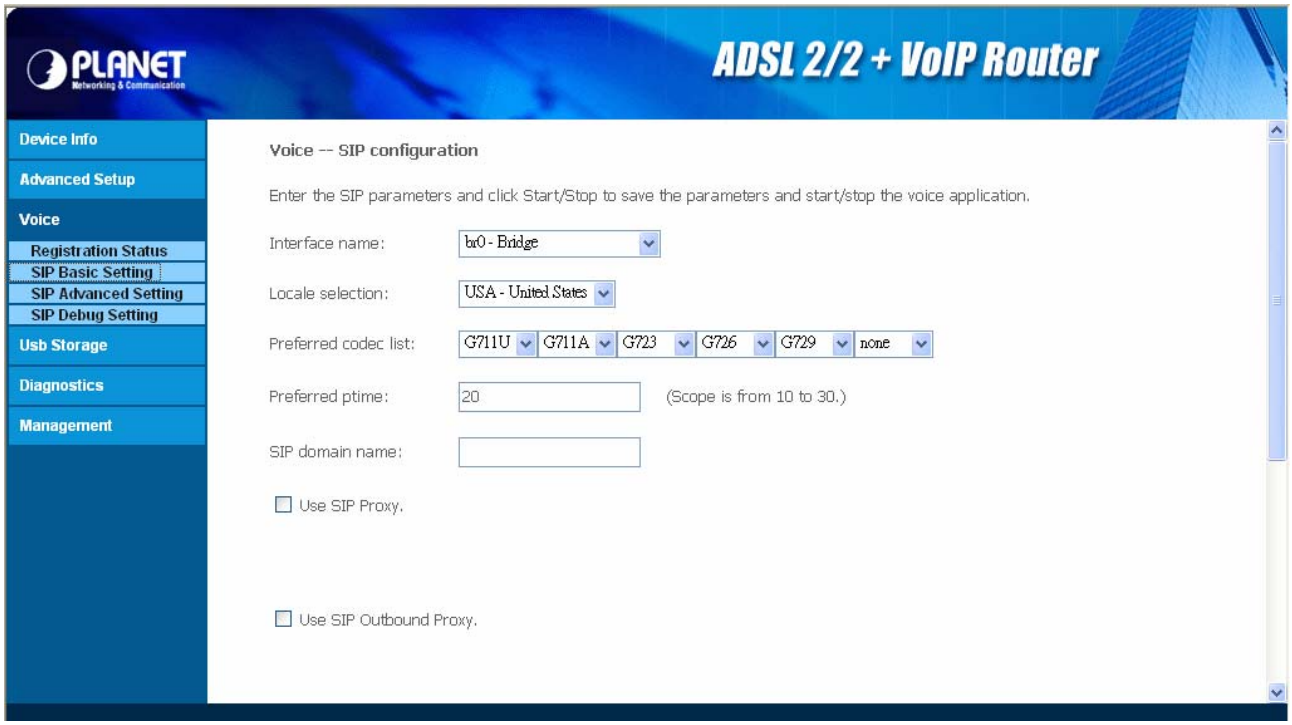


Figure: SIP Basic Setting Web Page

“SIP Basic Setting” web page enables you to set some parameters, such as Preferred codec list, Preferred ptime, SIP domain name and so on. The followings will show you how to configure the SIP Basic Setting Web Page step by step.

Interface name

Figure: Interface Name

This item provides for you to choose the way which DSL Router’s VoIP connect to SIP Proxy. There are two ways: br0-Bridge, PPPOE. If you do not configure the ‘Wan’ tab under the ‘Advanced Setup’ menu, there is only br0-Bridge you can choose. Default value is br0-Bridge. The method which you would like choose, please consult your Internet Service Provider (ISP).

Locale selection

Figure: Locale selection

This item provides for you to choose country where your locale in. The different country use different standards used by DSL ROUTER VoIP module, such as ring tone standard. Locale selection default value is USA.

Preferred code list

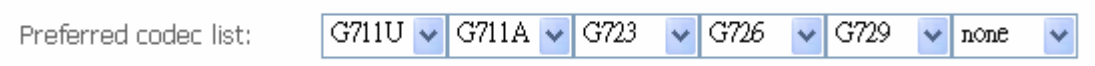


Figure: Preferred codec list

This item provides for you to specify the priority of codec, and the priority of codec declined from left to right.
Codec define the method of relaying voice data. Different codec have different characteristics, such as data compression and voice quality. For Example, G.723 is a codec that uses compression, so it is good for use where bandwidth is limited but its voice quality is not as good compared to other codec such as the G.711.
If you specify none of the codec, using the default value showed as figure 1.5, the DSL ROUTER will choose the codec automatically.

Preferred ptime

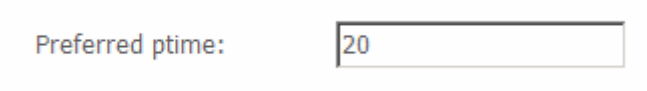


Figure: Preferred ptime

This item provides for you to set the Packetization Time (PT). The PT is the length of the digital voice segment that each packet holds. The default is 20 millisecond packets. If selecting 10 millisecond packets enhances the voice quality, as less information is lost due to packet loss, but doubles the load on the network traffic.

SIP domain name

Figure: SIP domain name

Fill in the SIP domain name or SIP server's IP address. If set to domain name, make sure it must be resolvable to SIP server's IP address.

Use SIP Proxy

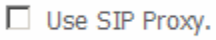


Figure: Use SIP Proxy

Select the check box if you DSL ROUTER uses a SIP proxy. SIP Proxy allows other parties to call DSL ROUTER through it. When this item is checked, the following fields appear:

Figure: SIP Proxy Parameters

SIP Proxy: Specify the proxy's IP address.
SIP Proxy port: The port that this proxy is listening on. Default port value is 5060.

Use SIP Outbound Proxy

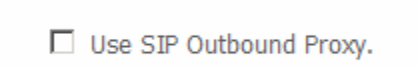


Figure: Use SIP Outbound Proxy

Some network service providers require the use of an outbound proxy. This is an additional proxy, through which all outgoing calls are directed. In some cases, the outbound proxy is placed alongside the firewall and is the only way to let SIP traffic pass from the internal network to the Internet. When this item is checked, the following fields become visible:

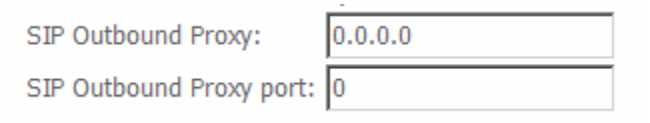


Figure: SIP Outbound Proxy parameters

SIP Outbound Proxy: The Outbound Proxy's IP address
SIP Outbound Proxy port: The port that the Outbound Proxy is listening on.

Use SIP Registrar

Figure: Use SIP Registrar

Select this option to register with the proxy. You can register your USER ID on the SIP Registrar. SIP Registrar works with SIP Proxy, allowing other parties to call DSL ROUTER through it. When this item is checked, the following field becomes visible:

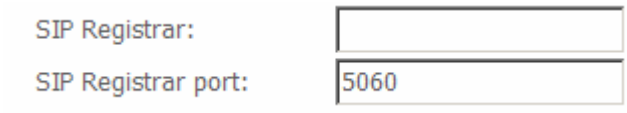


Figure: Use SIP Registrar Parameters

SIP Registrar: The SIP Registrar's IP address.
SIP Registrar port: The port that SIP Registrar is listening on. Default value is 5060.

Line Settings

Figure: Line Settings

There are five options you can checked or filled in:

- **Line Disabled:** Line number is a telephone port in DSL ROUTER to which you can connect a standard (POTS) telephone. If you checked this option, and the line corresponding you checked will be disable. You can not use it to initiate or accept any call.
- **Extension:** This is telephone's VoIP **user ID**, used for identification to initiate and accept calls.

- **Display Name:** A free text description which will be displayed to remote parties as your caller ID.
- **Authentication Name:** The login name used for authentication with the SIP proxy.
- **Password:** The password used for authentication with the SIP proxy.

NOTE: if you have **entered/changed** the parameters on the web site, you must click **Start/Sop** to save the parameters and **Start/Stop** the voice application.

3.4.2 SIP Advanced Setting

The advanced setting page contains those parameters that are not usually used. If you need advanced feature, such as FAX and MOH (Music on Hold), you can configure it here.

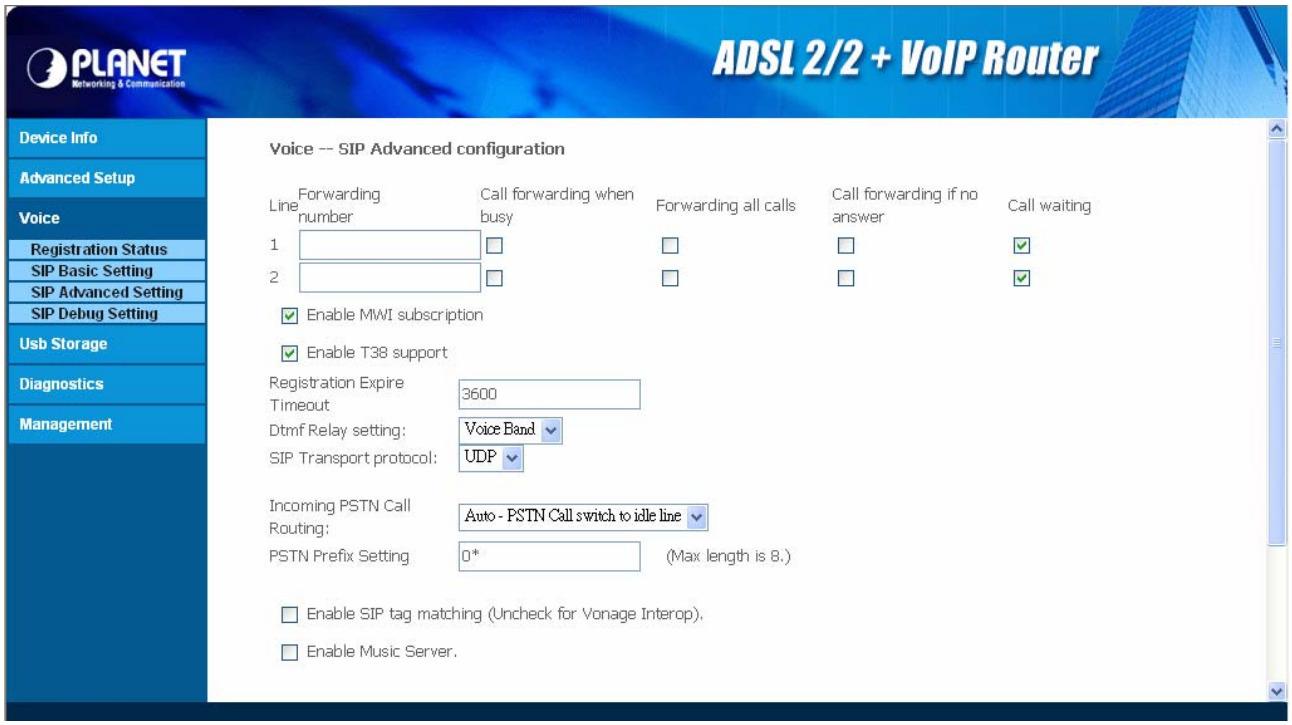


Figure: SIP Advanced Setting

Advanced Feature Setting

Figure: Advanced Feature Setting

Forwarding number:

Set the number to forward a call. This number can also be set through dialing '***74<NUM>#**' on the phone key pad.

Call forwarding when busy

Enable 'Call forwarding when busy' feature. When this box is checked, incoming calls will be forwarded when the specific line is busy. It has the same effect as dialing '***72**' on the phone pad.

Forwarding all calls

Enable 'Call forwarding all' feature. When this box is checked, incoming calls will be forwarded unconditionally. Dialing '***73**' can also accomplish this aim.

Call forwarding if no answer

Enable ‘Call forwarding no answer’. When this box is checked, incoming calls will be forwarded when it’s not answered in 18s. Dialing ‘***71**’ also makes it.

Call waiting

Enable ‘Call waiting’ feature on this line.

Enable MWI subscription

MWI stands for Message Waiting Indicator. When set this enabled, DSL ROUTER will send a SIP SUBSCRIBE message to proxy, asking for a notification when its voicemail status changes. When its status do changes, proxy will send a NOTIFY message to gateway, causing a MWI tone streamed to user’s handset.

Enable T38 support

Checking this box will enable T38 support. When doing a fax transmission on DSL ROUTER, after fax tone been detected, fax transmission will switch to T38 mode.

Registration Expire Timeout

It’s the interval DSL ROUTER will initiate a new registration since last one. It’s also known as ‘registration assurance timer’. Gateway uses this mechanism to keep its binding record updated.

Dtmf Relay setting

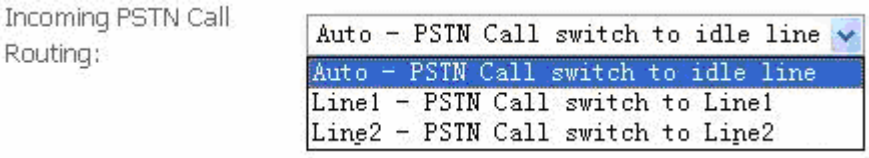
Set DTMF transmit method, which can be following values:

- **SIP Info:** Use SIP INFO message to transmit DTMF digits.
- **RFC2833:** Use RTP packet to encapsulate DTMF events, as specified in RFC 2833.
- **Voice Band:** DTMF events will be mixed with user voice in RTP packet.

SIP Transport protocol

Select the transport protocol to use for SIP signaling. Note SIP proxy and registrar need to support the protocol you choose.

Incoming PSTN Call Routing


Incoming PSTN Call Routing:
Auto - PSTN Call switch to idle line
Auto - PSTN Call switch to idle line
Line1 - PSTN Call switch to Line1
Line2 - PSTN Call switch to Line2

Select the way incoming PSTN calls to be routed. It has following items:

- **Auto - PSTN Call switch to idle line**

DSL ROUTER will automatically select the idle line for incoming PSTN call.

- **Line1 - PSTN Call switch to Line1**

PSTN call will be routed to line 1. If it's busy, PSTN call will fail.

- **Line2 - PSTN Call switch to Line2**

PSTN call will be routed to line 2.

Enable SIP tag matching

Enable the checking of the 'to' tag in SIP message. Enabling this feature may impose more strict checking on SIP messages. If you place DSL ROUTER in a Vantage network, using the Vantage server, make sure to uncheck it.

Enable Music Server

When set enabled, the holding party will act like a coordinator, and trigger the music server to stream music to the hold party. This is done by sending an INVITE without SDP to music server, and acknowledging server's response with an ACK message containing the SDP of the hold party. Music server then streams music to hold party.
Fill 'Music server' area with server's IP address, and specify the port in 'Music server port'.

3.4.3 VoIP functionality

This section will guide you how to use the functionality of DSL ROUTER in more detail. Some features involve 2 or 3 parties. In that case, note that all 3 parties have to be successfully registered.

Registering.

Before using any VoIP functionality, DSL ROUTER has to register itself to a registrar. DSL ROUTER also has to be configured with a proxy, which relays VoIP signaling to next hop. In fact, many implementations integrate these two into one server, so in many case registrar and proxy refer to the same IP.

1. Select the right interface to use for registering, depending on where Proxy/Registrar resides. If use WAN link, make sure it's already up.
2. Fill 'SIP domain name' with SIP proxy's IP address or domain name. Note if we use domain name, it must be resolvable to proxy's IP address.
3. Mark 'Use SIP Registrar' box, and fill below IP/Port field with the right value.
4. Fill the extension information: 'Extension', 'Display Name', 'Authentication Name' and 'Password'. 'Authentication Name' and 'Password' must be pre-configured in registrar database
5. Click 'Stop SIP client' (if VoIP application has been started already), then 'Start SIP client' to make above settings take effect.
6. VoIP LED should light on; indicating SIP client is successfully registered.

Placing a call

This section depicts how to place a basic VoIP call.

- Pick up the handset on the phone.
- Now you hear the dial-tone. Dial the extension of remote party
- To end the dialing, wait for digit-timeout or just press '#' immediately.
- After remote party answers the call, you're in voice connection.

Anonymous call

Anonymous call won't send the caller ID to remote party. This is useful if you don't want others know whom you are.

- Pick up the handset on the phone.
- Dial '***83**' to enable anonymous call.
- Hook on the handset, and dial another extension as you like. Now your caller ID information is blocked.
- To enable caller ID transmission again, dial '***84**' on the key pad.

Do not disturb (DND)

If DND enabled, all incoming calls will be rejected. DND is useful if you don't want others to bother you.

- Pick up the handset on the phone.
- Dial '***86**' to enable DND function
- Hook on the phone. Now your phone will reject all incoming calls.
- To disable DND, press '***87**' on the key pad.

Redial.

For outgoing calls, DSL ROUTER will remember the number you dial. Next time when you want to dial that person, DSL ROUTER provides you the redial functionality.

- To re-dial the latest dialed person, press '***68**' on the key pad.
- Now you have made the call, as if you just dialed the whole number.

Call return.

For incoming calls, DSL ROUTER remembers the number of calling party.

- To return a call, press **'*69**'
- Now you have made the call as if you have dialed the whole number

Call hold

Call hold enable you put a call to a pending state, and pick it in future.

- Assuming you are in a voice connection, you can press '**FLASH**' to hold current call.
- Now you can call another party, or press **'FLASH**' again to return to first call.

Call waiting.

Enabling call waiting will allow third party to call in when you're in a voice connection.

- Pick up the phone attached to DSL ROUTER.
- Press **'*61**' to enable call waiting function.
- Assuming you're in a voice connection, when another call comes in, DSL ROUTER will stream a call waiting tone to your phone, indicating another call is available.
- Press '**FLASH**' will switch to this call and the initial call will put to hold automatically.
- Press '**FLASH**' multi-times will switch between these two calls back and forth.
- Pressing '***60**' will disable call waiting function.

Blind transfer

Bind transfer will transfer the current call to a third party blindly, regardless of whether the transfer is successfully or not.

- Assume you have already been in a voice connection.
- Press '**FLASH**' to hold the first party.
- Dial a third party.

- Before the third party answers the call, hook on your phone.
- Now the first party takes over the call and is in connection with the third party.

Consultative transfer

Consultative transfer will let the third party answer the transferred call, and then hook on the transferring party. It' more gentle than blind transfer.

- Assume you have already been in a voice connection with a first party.
- Press '**FLASH**' to hold the first party.
- Dial a third party.
- After the third party answers the call, hook on your phone.
- Now the first party takes over the call and is in connection with the third party.

Call forwarding no answer

If this feature enabled, incoming calls will be forwarded to third party when you doesn't answer them. It involves two steps: setting the forwarding number and enable the feature.

- Dial '***74<NUM>#**' to set forwarding number, where 'NUM' is the number of the party whom the call is forwarded to.
- Dial '***71**' to enable call forwarding no answer. That is, when our phone doesn't answer incoming call, this call will be forwarded.
- Press '***70**' will disable call forwarding no answer.

Call forwarding busy

If this feature enabled, incoming calls will be forwarded to third party when you busy. It involves two steps: setting the forwarding number and enable the feature.

- Dial '***74<NUM>#**' to set forwarding number, where 'NUM' is the number of the party whom the call is forwarded to. Note if we have already set forwarding number before, this step can be omitted.
- Press '***72**' to enable call forwarding busy. That is, when our phone gets busy, this call will be forwarded.
- Press '***70**' will disable call forwarding busy.

Call forwarding all

If this feature enabled, incoming calls will be forwarded to third party without any reason. It involves two steps: setting the forwarding number and enable the feature.

- Dial '***74<NUM>#**' to set forwarding number, where 'NUM' is the number of the party whom the call is forwarded to. Note if we have already set forwarding number before, this step can be omitted.
- Press '***73**' to enable call forwarding all. That is, all incoming alls will be forwarded to the third party.
- Press '***75**' will disable call forwarding all, but let call forwarding no answer and call forwarding busy unchanged.

- Press '***70**' will disable all call forwarding function.

3-Way conference

3-way conference enables you to invite a third party to a call, and every person in the conference is able to hear others' voice.

- Assume you are in connection with a first party.
- Press '**FALSH**' to put the first party on hold.
- Dial a third party.
- After the third party answers the call, press '**FLASH**' again to invite the first party.
- Now all three parties are in a 3-way conference.

T38 Faxing

To make T38 faxing, enable T38 support on the web. After that, connect a fax machine to a FXS port of DSL ROUTER. Now you can treat it as a normal phone and is able to send or receive fax to or from other fax machines on the VoIP network.
In initial setup, faxing behaves like a normal call. After DSL ROUTER detects the fax tone, it switch to T38 mode, and use it as the transmit approach.

Pass-through Faxing

If T38 support is not enabled, faxing will use normal voice codec as its coding approach. So this mode looks much like normal phone calls.

PSTN to VoIP call

For incoming PSTN call, DSL ROUTER can route it to local FXS-attached analog phones or other VoIP extension, depending on the setting. In 'Voice/SIP Advanced Setting', there are four schemes in 'Incoming PSTN call routing' drop list:

Auto - PSTN Call switch to idle line
DSL ROUTER will automatically select the idle line for incoming PSTN call.

Line1 - PSTN Call switch to Line1
PSTN call will be routed to line 1. If it's busy, PSTN call will fail.

Line2 - PSTN Call switch to Line2
PSTN call will be routed to line 2.

3.5 USB Storage

We Access the USB Storage device on **USB1 Port** of DSL router, we must use FTP Protocol to operate USB device, and there are two functions in this chapter:

1. **FTP Server function:** LAN side PC can logon to operate USB file
2. **FTP Client function:** Can download file from internet to USB.

3.5.1 FTP Server Configure

FTP: FTP (File Transfer Protocol) is a protocol for exchanging files on the Internet. The standard Internet protocol for downloading, or transferring, files from one computer to another. You can use this standard, for example, to offer files for downloading or to receive files from other users.

Setting Parameters and configure example

FTP Listening Port: The default FTP Listening Port is 21; here the user can modify the port value.

Max Connections for the same IP: It means the max connections the user going to set, note that 0 means no restrict. It connects automatically.

FTP Account Management: There are three levels account, **ftpadmin** account has the biggest authority, it can view, download and upload files. **ftpuser** account can view and download files. **anonymous** account only has the view authority.

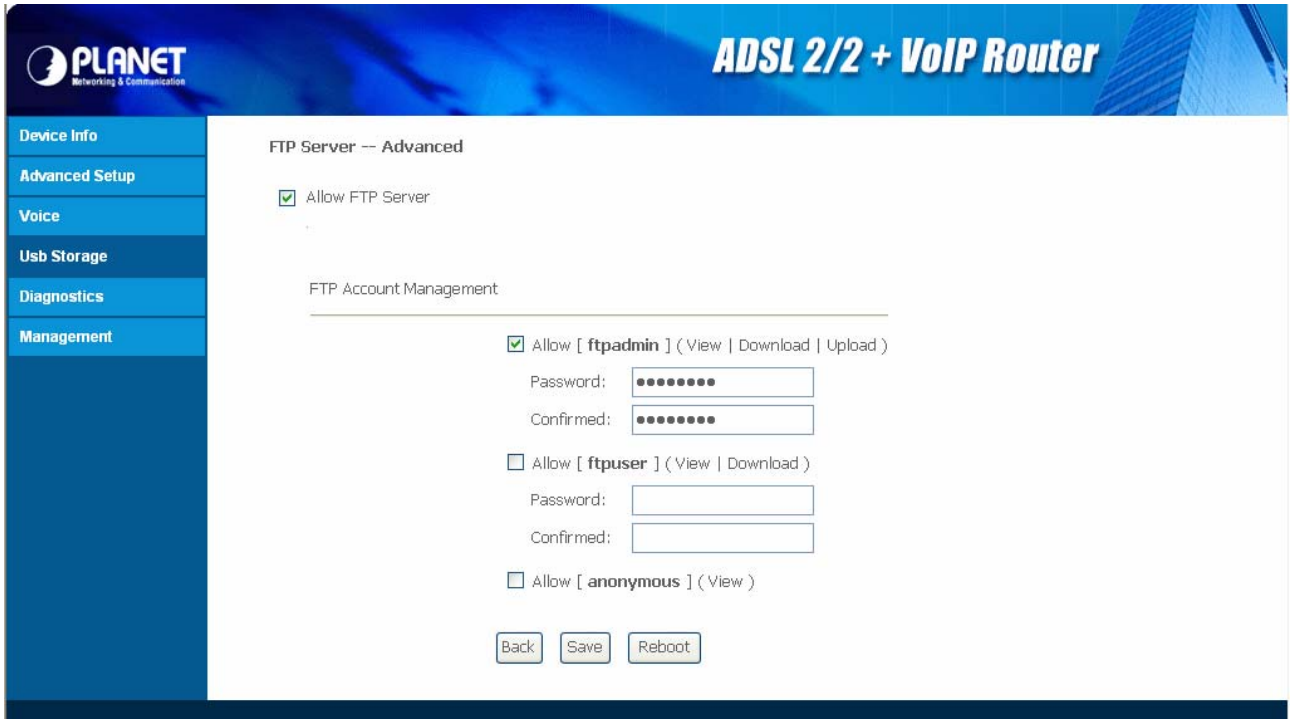


Figure: FTP Server Config

Note: After click “save” button, you need to reboot the Router to activate this setting.

3.5.2 FTP Client Setting

Local Path: When you insert USB storage, it will show the USB storage information to us, and you can select which storage to store.

Username: The account name which is set in the FTP Server Configure WEB UI.

Password: The same with above.

Port: The same with above.

Remote URL: It is the remote FTP address where you are going to download files. When we download files, we store it to Local Path.

The following is the example how to configure the setting.

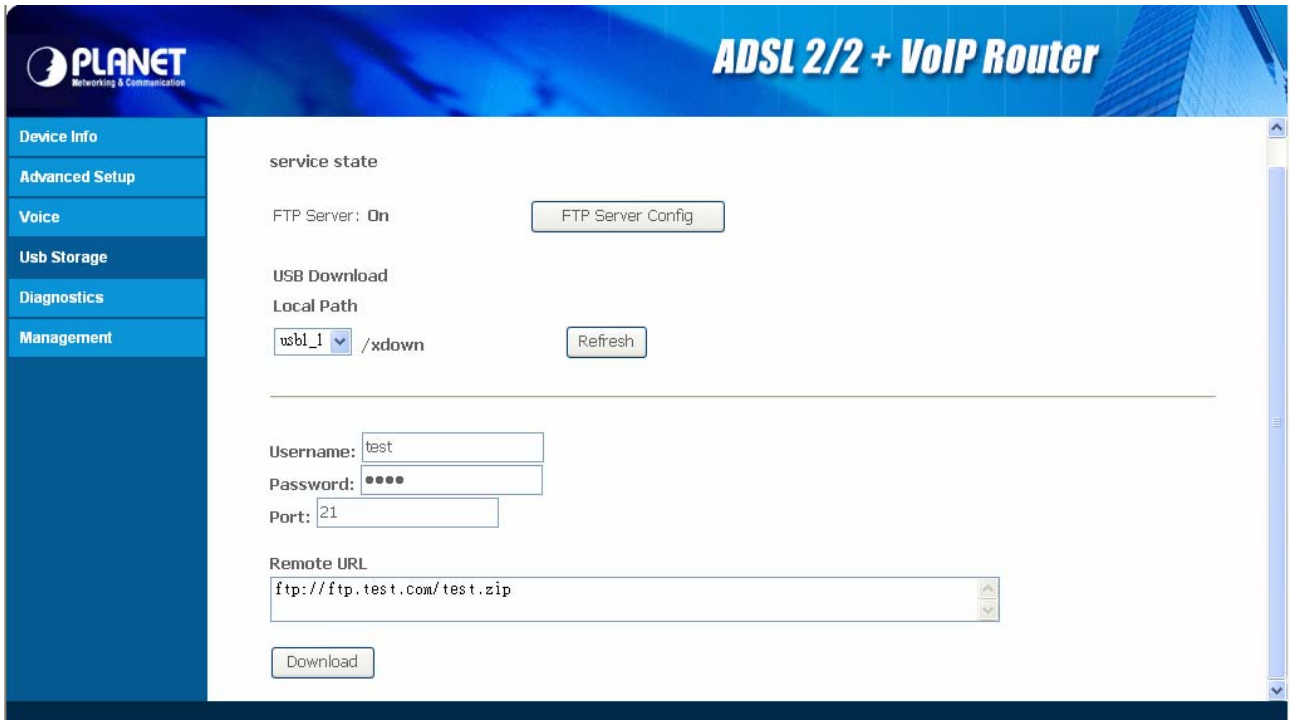


Figure: Ftp client Setting

3.6 Diagnostics

Click “Diagnostics” to show the interface.

Your Router is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

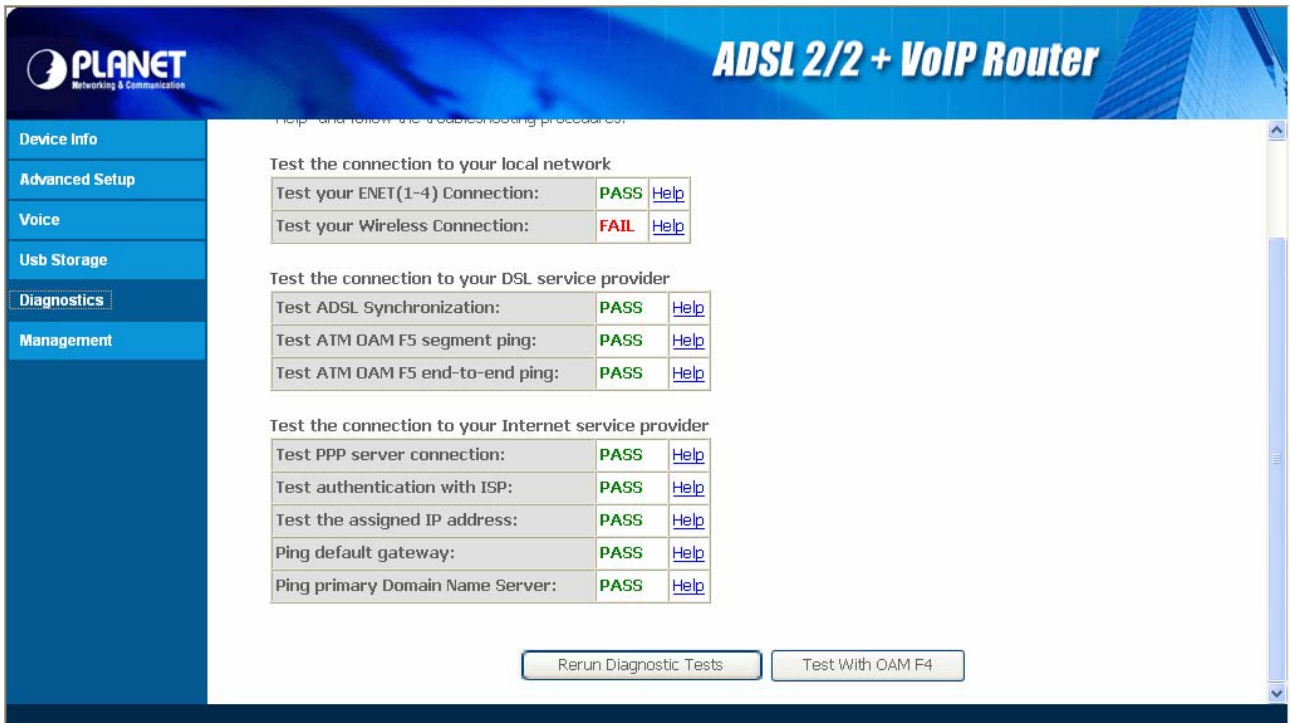

PLANET
Networking & Communication
ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
Voice
Usb Storage
Diagnostics
Management
Test the connection to your local network
Test your ENET(1-4) Connection: PASS Help
Test your Wireless Connection: FAIL Help
Test the connection to your DSL service provider
Test ADSL Synchronization: PASS Help
Test ATM OAM F5 segment ping: PASS Help
Test ATM OAM F5 end-to-end ping: PASS Help
Test the connection to your Internet service provider
Test PPP server connection: PASS Help
Test authentication with ISP: PASS Help
Test the assigned IP address: PASS Help
Ping default gateway: PASS Help
Ping primary Domain Name Server: PASS Help
Rerun Diagnostic Tests
Test With OAM F4

Figure: Diagnostics page

3.7 Management

3.7.1 Settings

3.7.1.1 Settings Backup

Click the “Backup Settings”, backup the DSL router configurations.

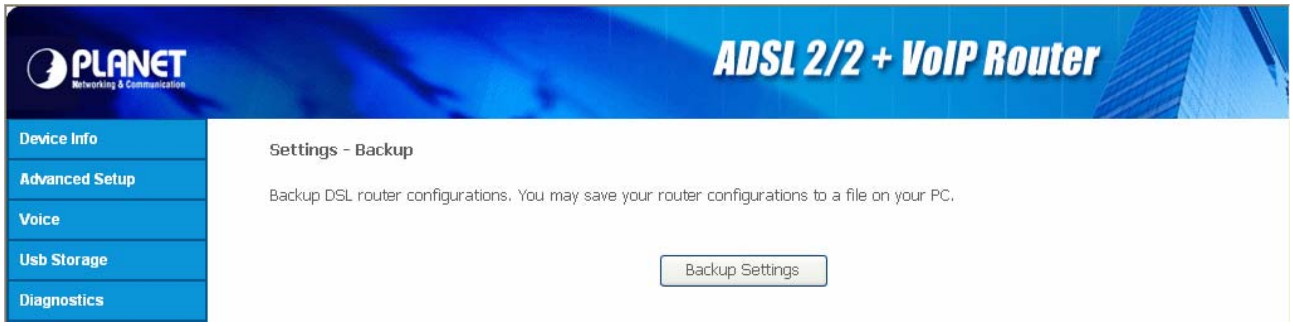


Figure: Backup Config

3.7.1.2 Settings Update

Click the “Browsing...” button, select the correct update configure settings file. Then click the “Update Settings” to update the Router settings.

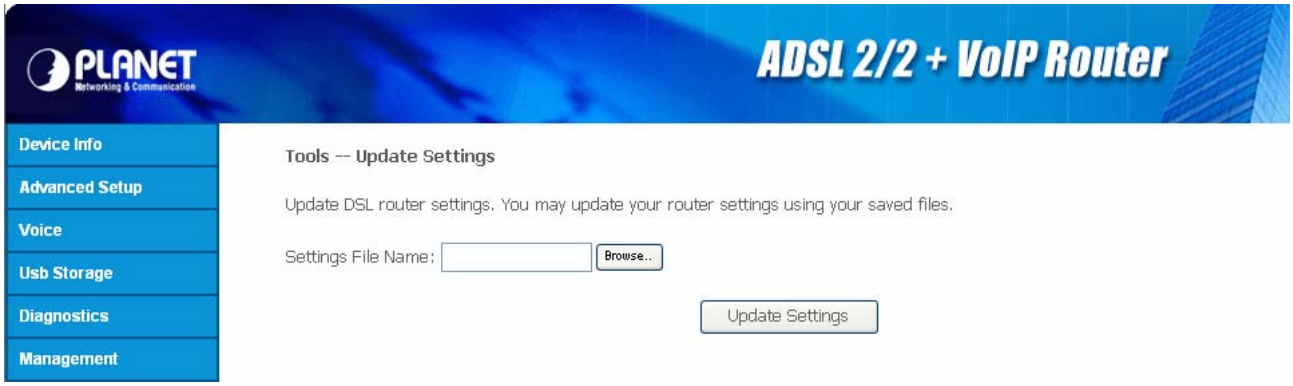


Figure 3.5.10: Update Settings

3.7.1.3 Settings Restore Default

Click “Restore Default Settings” to restore DSL router settings to the factory defaults.

Figure: Restore Default Settings

3.7.2 System Log

Click “System Log” to show the following interface. The system log dialog allows you to view the system log and configure the system log options.

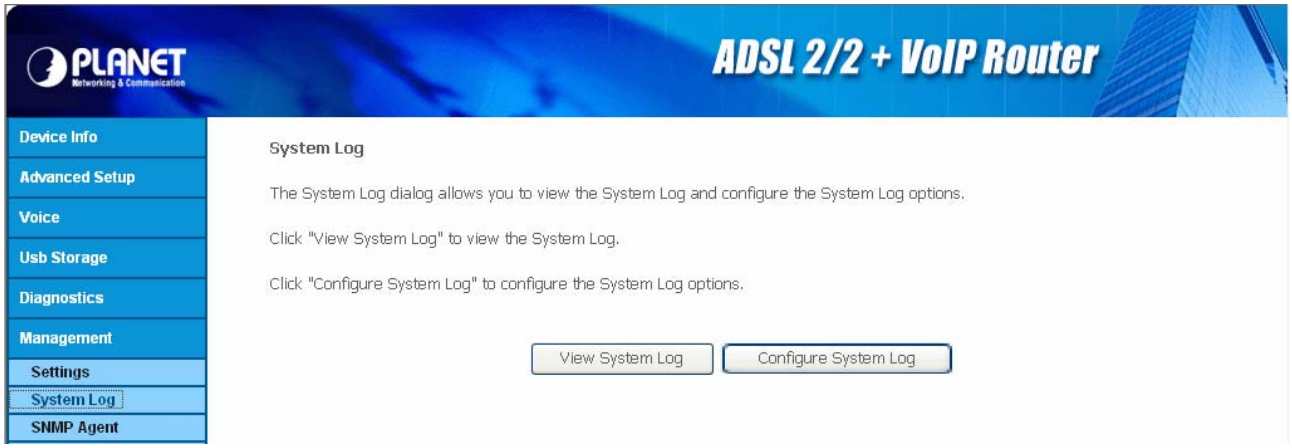
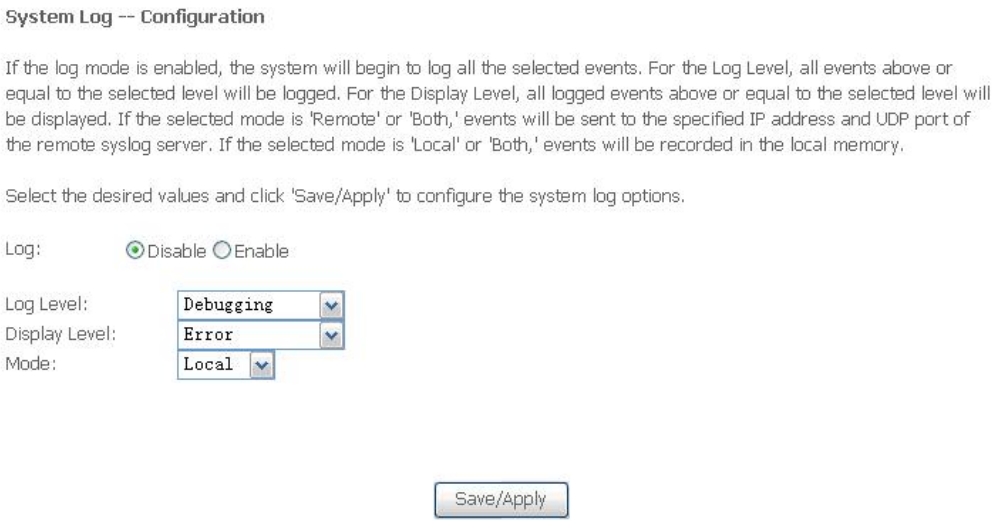


Figure: System Log overview

Click “Configure System Log” to show the following interface. You can enable or disable the system log and then select the log level, display level and mode, and click “Apply” to end your configurations.


System Log -- Configuration
If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.
Select the desired values and click 'Save/Apply' to configure the system log options.
Log:
Disable
Enable
Log Level:
Debugging
Display Level:
Error
Mode:
Local
Save/Apply

Both the log level and display level have eight choices. The default log level is “Debugging” and the default display level is “Error”.

The mode options are “Local”, “Remote”, and “Both”. The default one is “Local”.

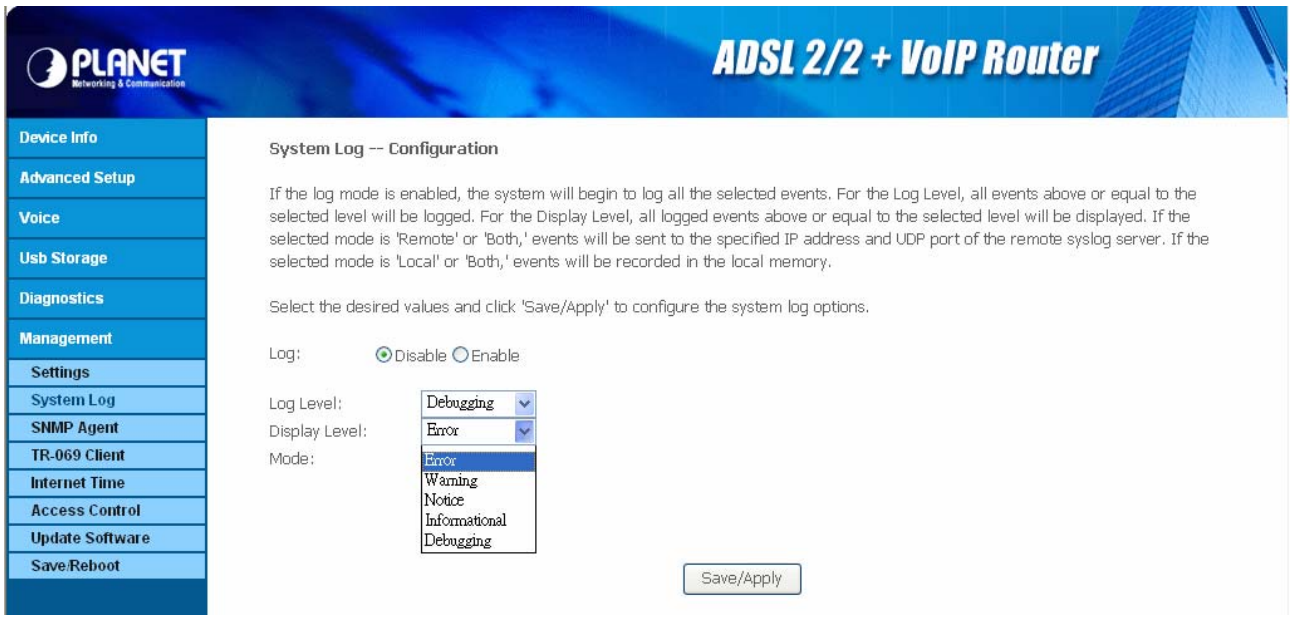

PLANET
ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
Voice
Usb Storage
Diagnostics
Management
Settings
System Log
SNMP Agent
TR-069 Client
Internet Time
Access Control
Update Software
Save/Reboot
System Log -- Configuration
If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.
Select the desired values and click 'Save/Apply' to configure the system log options.
Log: Disable Enable
Log Level: Debugging
Display Level: Error
Mode:
Error
Warning
Notice
Informational
Debugging
Save/Apply

Figure: System Log Config-1

If you select “Remote” or “Both”, all events will be transmitted to the specified UDP port of the specified log server.

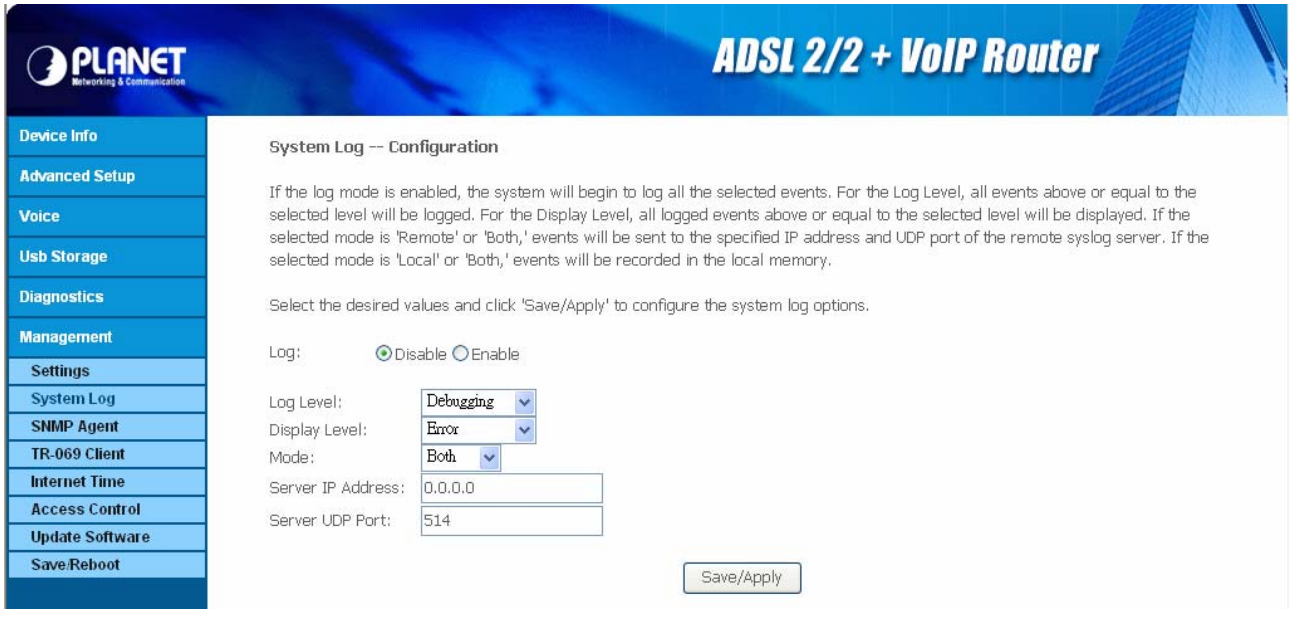

PLANET
ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
Voice
Usb Storage
Diagnostics
Management
Settings
System Log
SNMP Agent
TR-069 Client
Internet Time
Access Control
Update Software
Save/Reboot
System Log -- Configuration
If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.
Select the desired values and click 'Save/Apply' to configure the system log options.
Log: Disable Enable
Log Level: Debugging
Display Level: Error
Mode: Both
Server IP Address: 0.0.0.0
Server UDP Port: 514
Save/Apply

Figure: System Log Config-2

After operations under “Configure System Log”, click “View System Log” to query the system logs. In this example, the “View System Log” is a system default one.

Note: The log and display of the system events are above the set level. If you intend to record all information, you need to set the levels as “Debugging”.

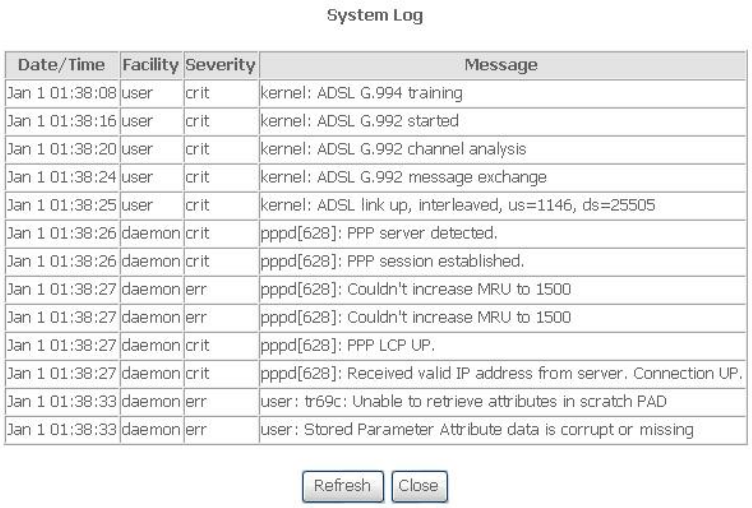

System Log
Date/Time
Facility
Severity
Message
Jan 1 01:38:08 user crit kernel: ADSL G.994 training
Jan 1 01:38:16 user crit kernel: ADSL G.992 started
Jan 1 01:38:20 user crit kernel: ADSL G.992 channel analysis
Jan 1 01:38:24 user crit kernel: ADSL G.992 message exchange
Jan 1 01:38:25 user crit kernel: ADSL link up, interleaved, us=1146, ds=25505
Jan 1 01:38:26 daemon crit pppd[628]: PPP server detected.
Jan 1 01:38:26 daemon crit pppd[628]: PPP session established.
Jan 1 01:38:27 daemon err pppd[628]: Couldn't increase MRU to 1500
Jan 1 01:38:27 daemon err pppd[628]: Couldn't increase MRU to 1500
Jan 1 01:38:27 daemon crit pppd[628]: PPP LCP UP.
Jan 1 01:38:27 daemon crit pppd[628]: Received valid IP address from server. Connection UP.
Jan 1 01:38:33 daemon err user: tr69c: Unable to retrieve attributes in scratch PAD
Jan 1 01:38:33 daemon err user: Stored Parameter Attribute data is corrupt or missing
Refresh
Close

Figure: view system event logs

Click “Refresh” to refresh the system event logs or “Close” to exit from this interface.

3.7.3 SNMP Client

SNMP Protocol

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

Two versions of SNMP exist: SNMP version 1 (SNMPv1) and SNMP version 2 (SNMPv2). Both versions have a number of features in common, but SNMPv2 offers enhancements, such as additional protocol operations. Figure 1 illustrates a basic network managed by SNMP.

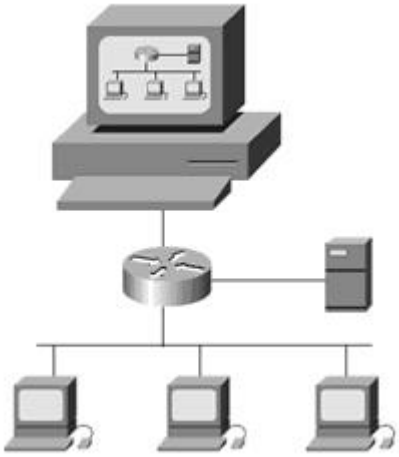


Figure1: SNMP Facilitates the Exchange of Network Information between Devices

An SNMP-managed network consists of three key components: managed devices, agents, and network-management systems (NMSs).

A managed device is a network node that contains an SNMP agent and that resides on a managed network. Managed devices collect and store management information and make this information available to NMSs using SNMP. Managed devices, sometimes called network elements, can be routers and access servers, switches and bridges, hubs, computer hosts, or printers.

An agent is a network-management software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP.

An NMS executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs must exist on any managed network.

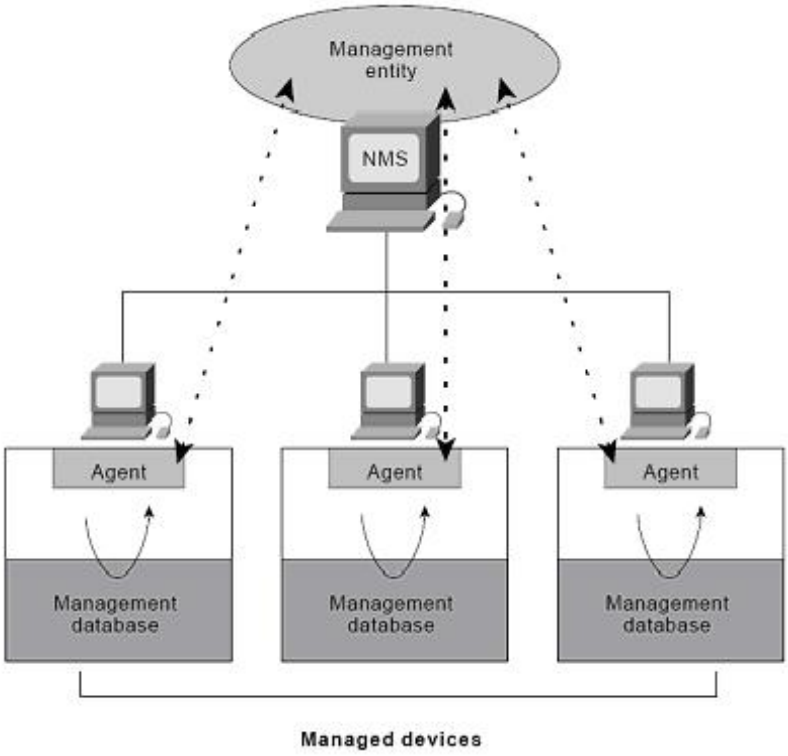


Figure2: An SNMP-Managed Network Consists of Managed Devices, Agents, and NMSs

Managed devices are monitored and controlled using four basic SNMP commands: read, write, trap, and traversal operations.

The ***read*** command is used by an NMS to monitor managed devices. The NMS examines different variables that are maintained by managed devices.

The ***write*** command is used by an NMS to control managed devices. The NMS changes the values of variables stored within managed devices.

The ***trap*** command is used by managed devices to asynchronously report events to the NMS. When certain types of events occur, a managed device sends a trap to the NMS.

Traversal operations are used by the NMS to determine which variables a managed device supports and to sequentially gather information in variable tables, such as a routing table.

Configure

Click “SNMP Agent” sub menu item under “Management” menu item, show figure 3 as following:

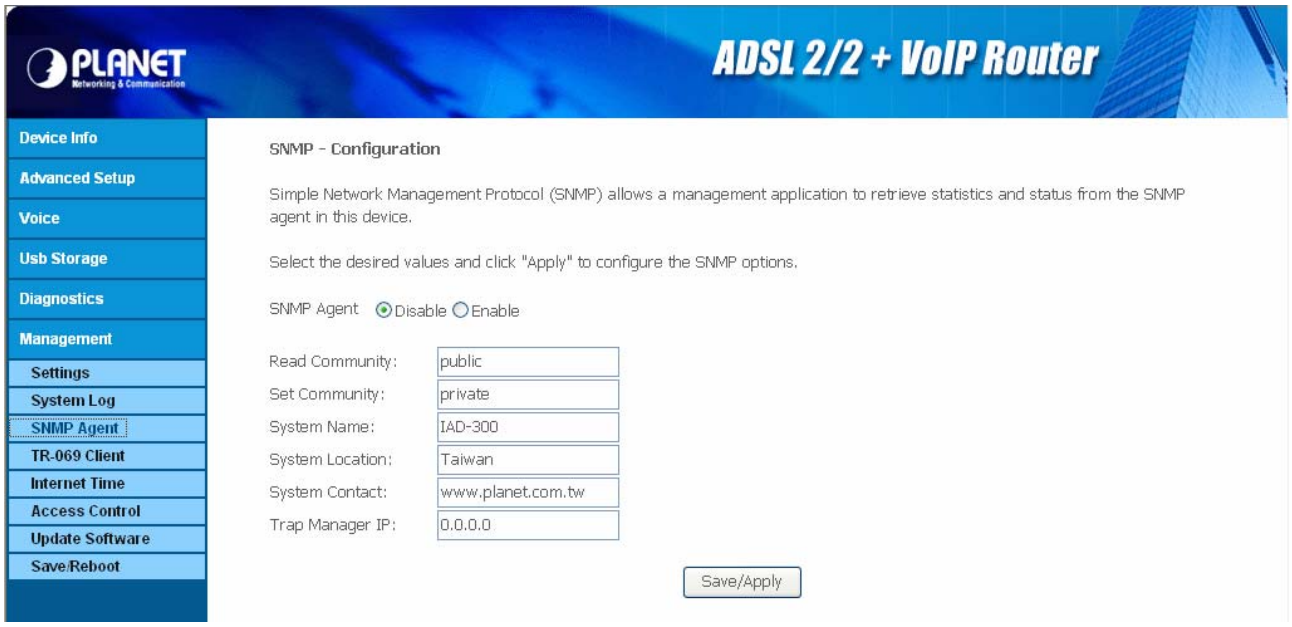


Figure: SNMP Config

Click “Enable” button to open SNMP function, and then click “Save/Apply”.

3.7.4 TR-69 Client Management

TR-069 Client-configuration

Click “Management” --> “TR-069Client” to show the **TR-069 Client** configuration page.

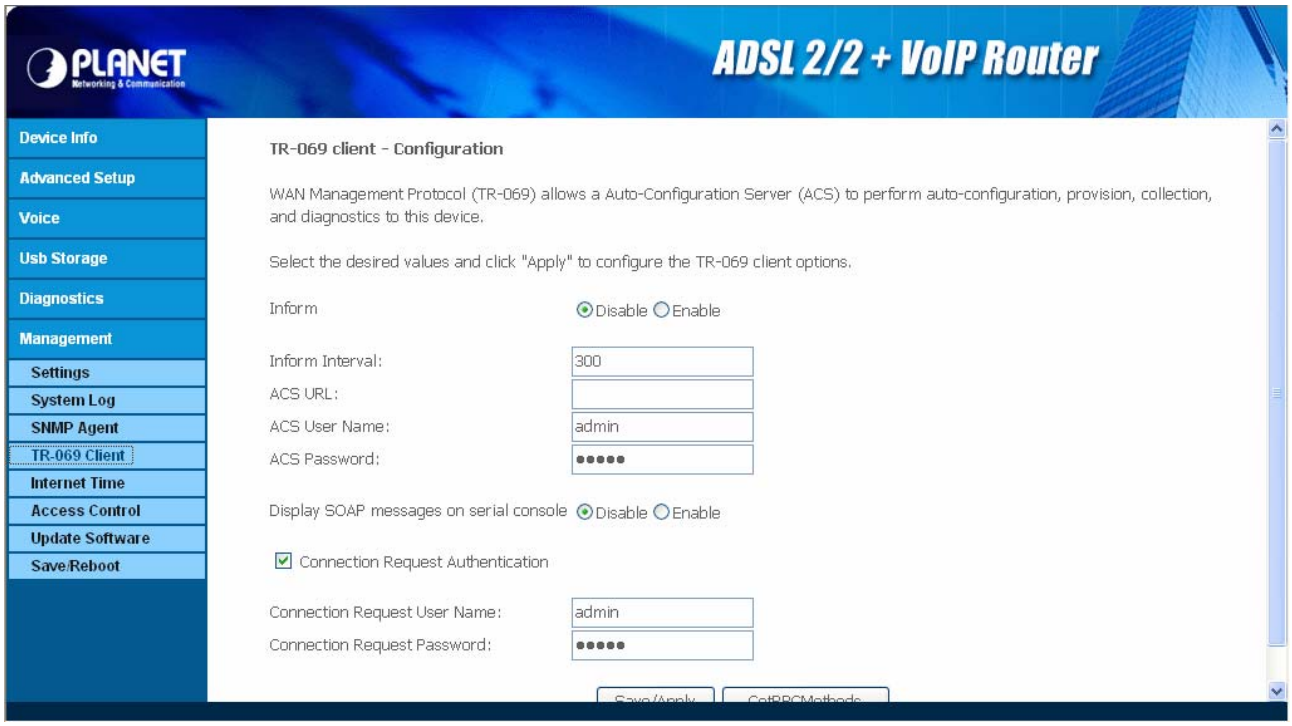


Figure: TR-069 Client Configuration

- **Inform:** IF the Enable option is selected,the CPE will accept the commands from ACS, the CPE will not accept the commands from ACS when the Disable option is selected.
- **Inform Interval:** How many seconds does the CPE inform the ACS to connect.
- **ACS URL:** input the ACS URL
- **ACS User Name:** The ACS user name is that the TR-069 Service provide to you.
- **ACS Password:** The ACS password is that the TR-069 Service provide to you.
- **Display SOAP messages on serial console:** When select Enable option, the SOAP information will display on the serial console, when select disable, it will not.
- **Connection Request Authentication:** If this checkbox is selected, you need to input the Connection Request User Name and the Connection Request Password. or you needn’t to input.
- **Connection Request User Name:** the connection user name that the TR-069 Service provide to you
- **Connection Request Password:** the Connection Request Password that the TR-069 Service provide to you.
- When Click “Save/Apply”, the configuration will save and apply.

3.7.5 Internet Time

Click the “Internet Time”, the interface show you. In this page, the ROUTER can synchronize with Internet time servers.

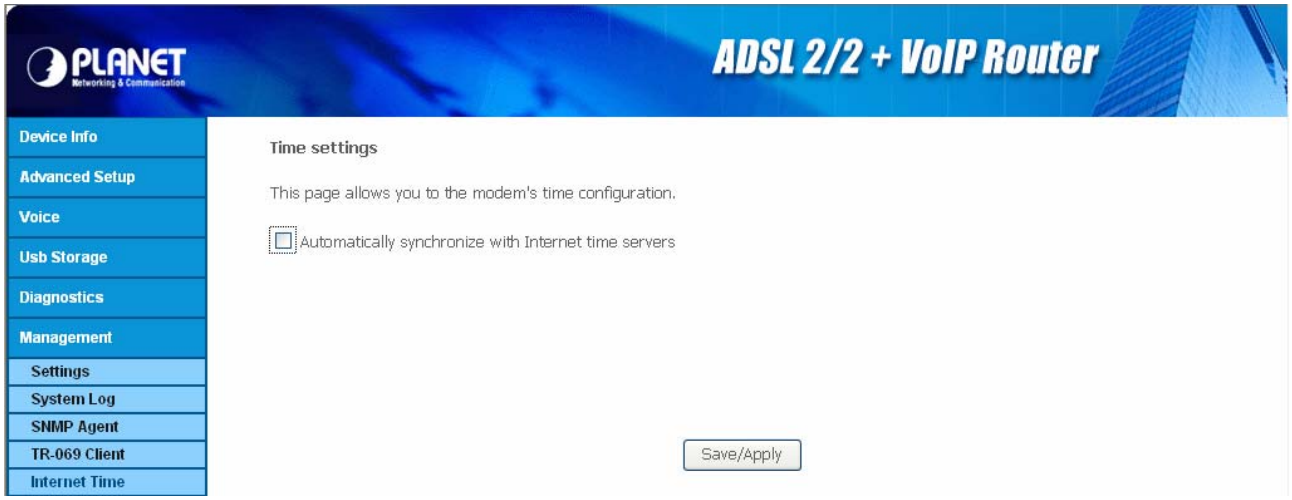


Figure: Internet Time overview

After enable “Automatically synchronize with Internet time servers.” the interface shows below. Enter proper configurations, and then click “Save/Apply”.

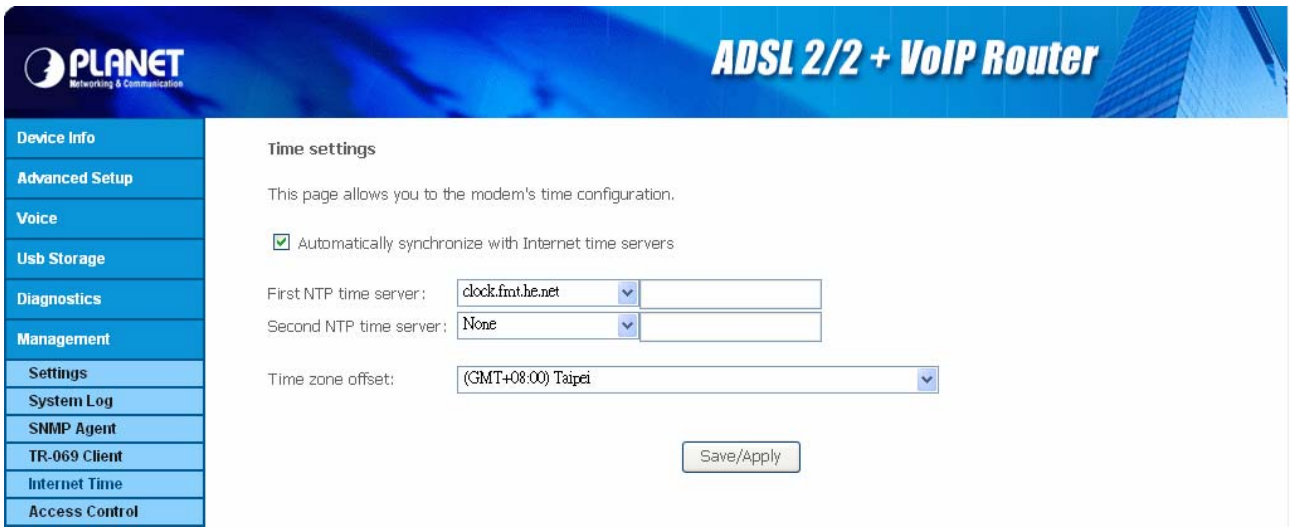


Figure: Internet Time Setup

3.7.6 Access Control

3.7.6.1 Access Control – Services

Click “Access Control”-->”Services” to show the following interface. In the interface, you can enable/disable the FTP, HTTP, ICMP, SSH, TELNET and TFTP services. And the LAN side and WAN side can have different configurations.

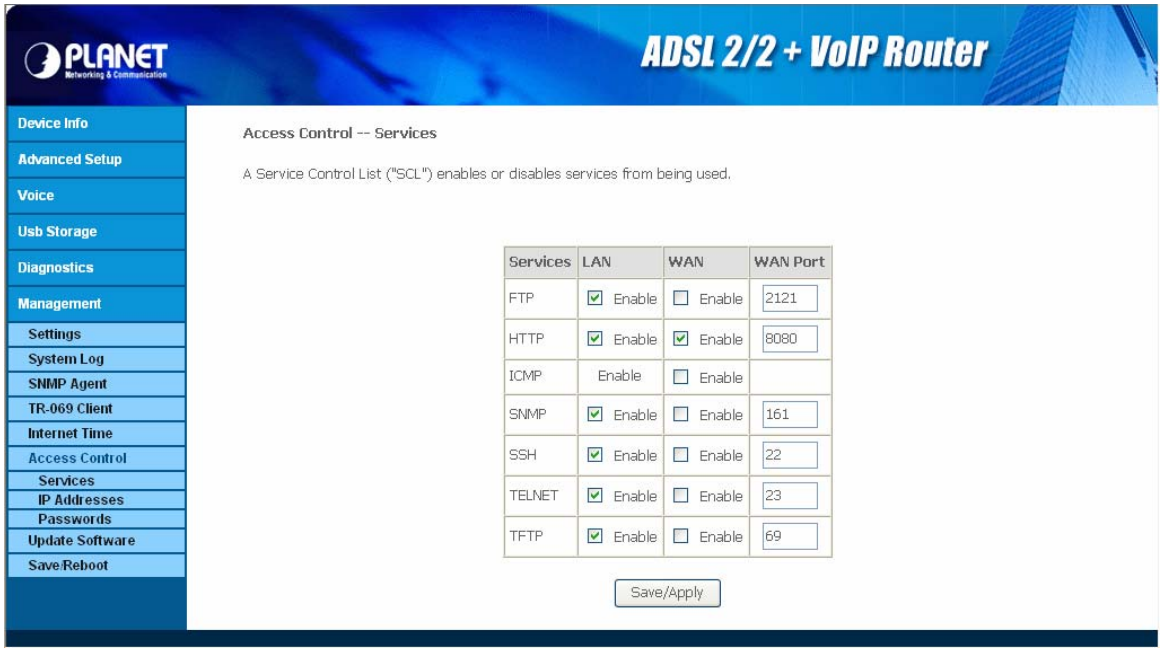


Figure: Access Control-Services Setup

3.7.6.2 Access Control -- IP Addresses

Click “Access Control”-->”IP Addresses” to show the following interface.

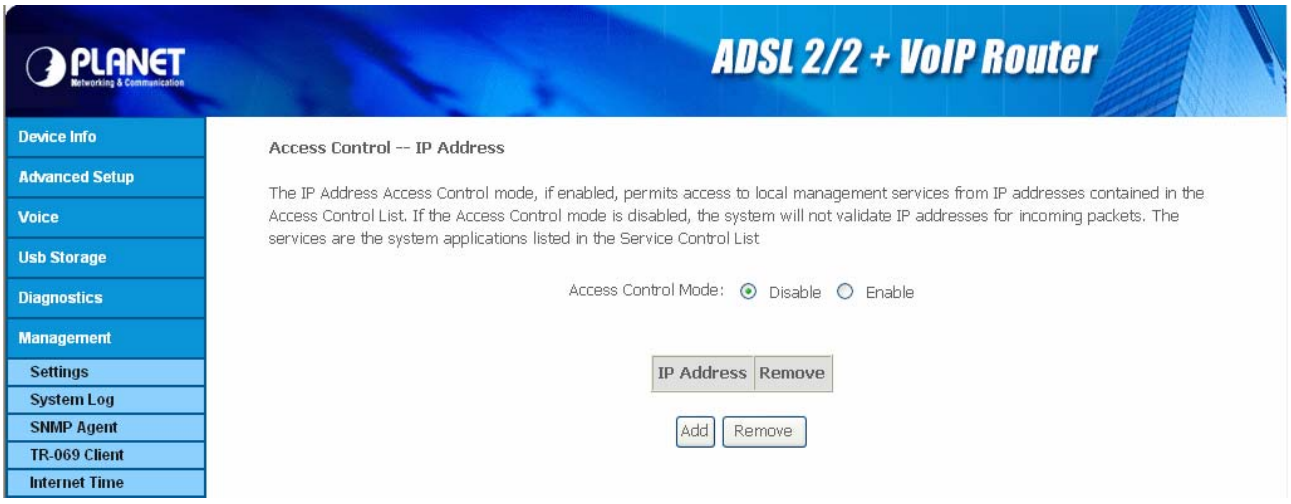

PLANET
ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
Voice
Usb Storage
Diagnostics
Management
Settings
System Log
SNMP Agent
TR-069 Client
Internet Time
Access Control -- IP Address
The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List
Access Control Mode: Disable Enable
IP Address Remove
Add Remove

Figure: Access Control-IP Addresses overview

If enabled, permits access to local management services from IP addresses contained in the Access Control List.

If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List.

Click “add” to show the following interface. In the interface input the IP address of the management station permitted to access the local management services, and click “Save/Apply”.

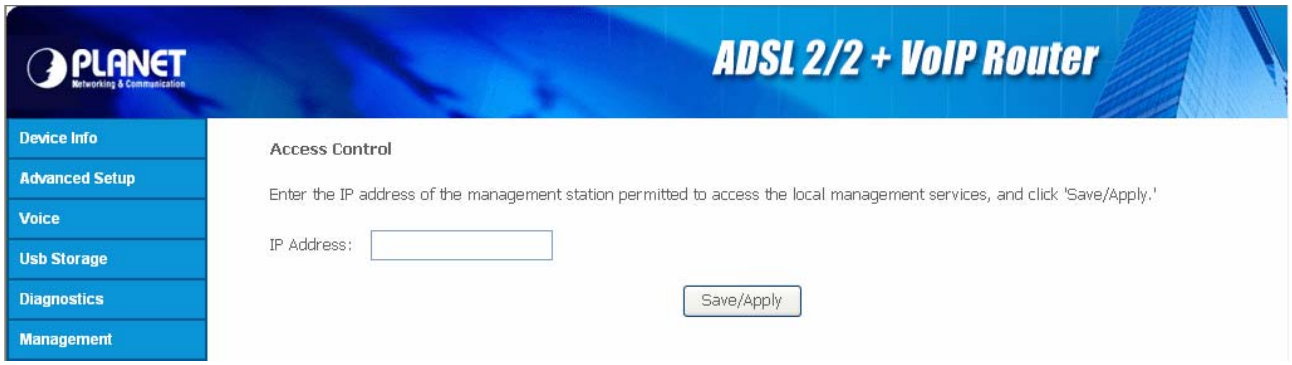


Figure: Access Control-IP Addresses

3.7.6.3 Access Control – Passwords

Click “Access Control”-->”Passwords” to show the following interface. In the interface, you can modify the accounts passwords.

Access to your DSL router is controlled through three user accounts: **admin, support, and user**

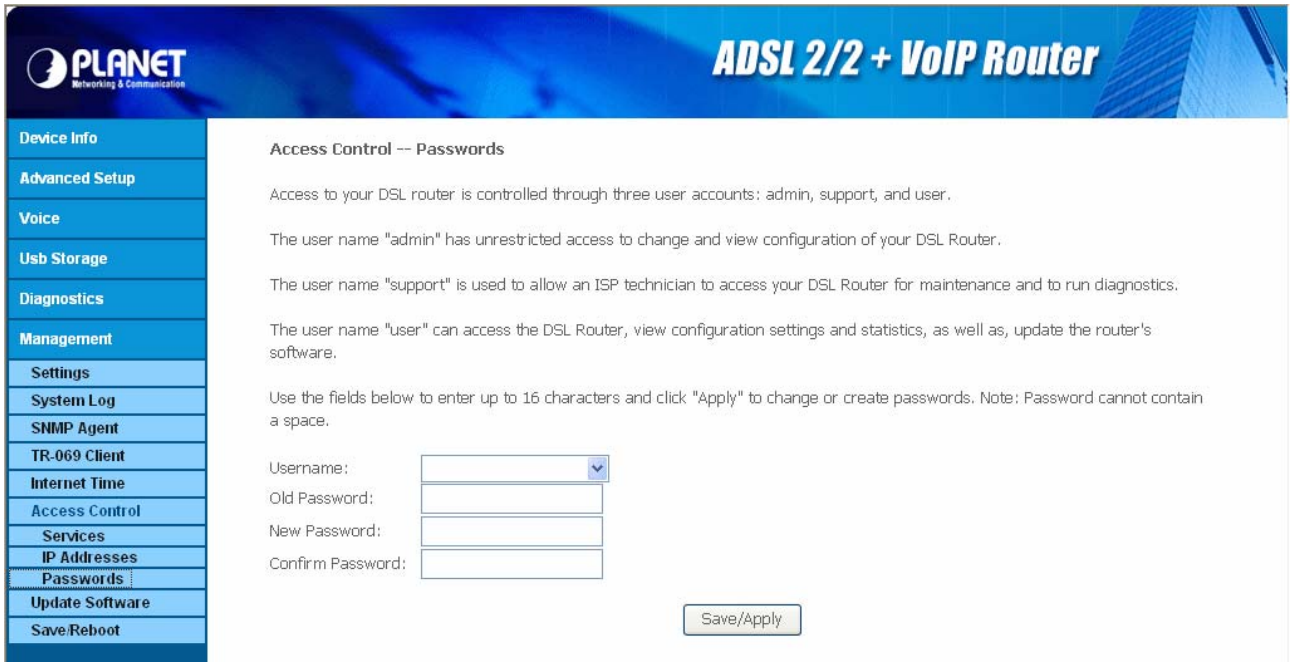

PLANET
Networking & Communication
ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
Voice
Usb Storage
Diagnostics
Management
Settings
System Log
SNMP Agent
TR-069 Client
Internet Time
Access Control
Services
IP Addresses
Passwords
Update Software
Save/Reboot
Access Control -- Passwords
Access to your DSL router is controlled through three user accounts: admin, support, and user.
The user name "admin" has unrestricted access to change and view configuration of your DSL Router.
The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.
The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.
Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.
Username:
Old Password:
New Password:
Confirm Password:
Save/Apply

Figure: Password modify page

3.7.7 Update Software

Click “Update Firmware” to show the following interface. In this interface, you can update the ROUTER Firmware. Click the “Browse...” button to find the right version file and press “Update Firmware” to do the update.

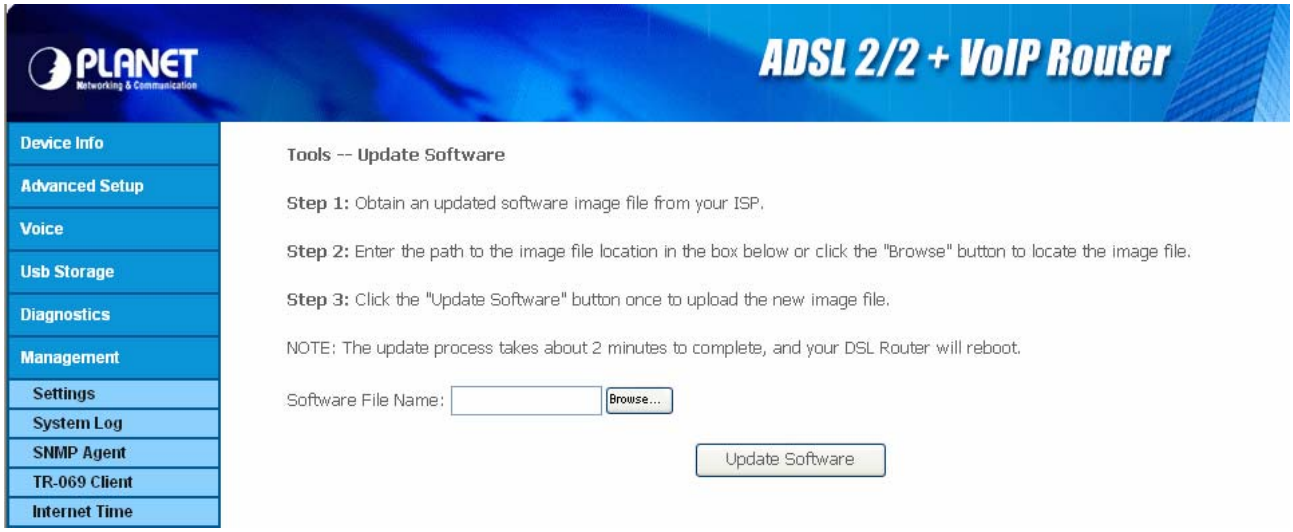

PLANET
ADSL 2/2 + VoIP Router
Device Info
Advanced Setup
Voice
Usb Storage
Diagnostics
Management
Settings
System Log
SNMP Agent
TR-069 Client
Internet Time
Tools -- Update Software
Step 1: Obtain an updated software image file from your ISP.
Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.
Step 3: Click the "Update Software" button once to upload the new image file.
NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.
Software File Name:
Browse...
Update Software

Figure: Update Software page

NOTE: Do not turn off your Router during firmware updates. When the update is finished, the Router will reboot automatically. Do not turn off your Router either before the reboot is over. You must guarantee the update software is right and accurate. It is strictly forbidden to use other software for updates.

After update software, it is suggested to restore the Router to the factory defaults and configure it again.

3.7.8 Save/Reboot

Click “Save/Reboot” to show the following interface. Click the “Save/Reboot” button to save and reboot the router.

Figure: Router Save/reboot page

Appendix A: Glossary

Address mask
A bit mask select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address
and one or more bits of the local portion. Sometimes it called subnet mask.

AAL5
ATM Adaptation Layer - This layer maps higher layer user data into ATM cells, making the data suitable for transport through the ATM network.

ADSL
Asymmetric digital subscriber line

ATM
Asynchronous Transfer Mode - A cell-based data transfer technique in which channel demand determines packet allocation. ATM offers fast packet technology,
real time, and demand led switching for efficient use of network resources.
AWG
American Wire Gauge - The measurement of thickness of a wire

Bridge
A device connects two or more physical networks and forward packets between them. Bridges can usually be made to filter packets, that is, to forward only certain traffic. Related devices are repeaters which simply forward electrical signals from one cable to the other and full-fledged routers which make routing decisions based on several criteria.

Broadband
Characteristic of any network multiplexes independent network carriers onto a single cable. Broadband technology allows several networks to coexist on one single cable; traffic from one network does not interfere with traffic from another. Broadcast a packet delivery system where a copy of a given packet is given to all hosts attached to the network. Example: Ethernet.

CO
Central Office. Refers to equipment located at a Telco or service provider's office.

CPE
Customer Premises Equipment located in a user's premises

DHCP (Dynamic Host Configuration Protocol)
DHCP is software that automatically assigns IP addresses to client stations logging onto a TCP/IP network. DHCP eliminates having to manually assign permanent IP addresses to every device on your network. DHCP software typically runs in servers and is also found in network devices such as Routers.

DMT
Discrete Multi-Tone frequency signal modulation

Downstream rate
The line rate for return messages or data transfers from the network machine to the user's premises machine.

DSLAM
Digital Subscriber Line Access Multiplex
Dynamic IP Addresses
A dynamic IP address is an IP address that is automatically assigned to a client station (computer, printer, etc.) in a TCP/IP network. Dynamic IP addresses are typically assigned by a DHCP server, which can be a computer on the network or another piece of hardware, such as the Router. A dynamic IP address
may change every time your computer connects to the network.

Encapsulation
The technique layer protocols in which a layer adds header information to the protocol data unit (PDU) from the layer above. As an example, in Internet terminology, a packet would contain a header from the physical layer, followed by a header from the network layer (IP), followed by a header from the transport
layer (TCP), and followed by the application protocol data.

Ethernet
One of the most common local area network (LAN) wiring schemes, Ethernet has a transmission rate of 10 Mbps.

FTP
File Transfer Protocol. The Internet protocol (and program) transfer files between hosts.

Hop count
A measure of distance between two points on the Internet. It is equivalent to the number of gateways that separate the source and destination.

HTML
Hypertext Markup Language - The page-coding language for the World Wide Web.

HTML browser
A browser used to traverse the Internet, such as Netscape or Microsoft Internet Explorer.

http
Hypertext Transfer Protocol - The protocol carry world-wide-web (www) traffic between a www browser computer and the www server being accessed.

ICMP
Internet Control Message Protocol - The protocol handle errors and control messages at the IP layer. ICMP is actually part of the IP protocol.

Internet address
An IP address is assigned in blocks of numbers to user organizations accessing the Internet. These addresses are established by the United States Department of Defense's Network Information Center. Duplicate addresses can cause major problems on the network, but the NIC trusts organizations to use individual addresses responsibly. Each address is a 32-bit address in the form of x.x.x.x where x is an eight- bit number from 0 to 255. There are three classes: A, B and C, depending on how many computers on the site are likely to be connected.

Internet Protocol (IP)
The network layer protocol for the Internet protocol suite

IP address
The 32-bit address assigned to hosts that want to participate in a TCP/IP Internet.

ISP
Internet service provider - A company allows home and corporate users to connect to the Internet.

MAC
Media Access Control Layer - A sub-layer of the Data Link Layer (Layer 2) of the ISO OSI Model responsible for media control.

MIB
Management Information Base - A collection of objects can be accessed via a network management protocol, such as SNMP and CMIP (Common Management Information Protocol).

NAT
Network Address Translation - A proposal for IP address reuse, where the local IP address is mapped to a globally unique address.

NVT
Network Virtual Terminal
PAP
Password Authentication Protocol

PORT
The abstraction used in Internet transport protocols to distinguish among multiple simultaneous connections to a single destination host.

POTS
Plain Old Telephone Service - This is the term describe basic telephone service.

PPP
Point-to-Point-Protocol - The successor to SLIP, PPP provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits.

PPPoE
PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

Remote server
A network computer allows a user to log on to the network from a distant location.

RFC
Request for Comments - Refers to documents published by the Internet Engineering Task Force (IETF) proposing standard protocols and procedures for the Internet. RFC can be found at www.ietf.org.

Route
The path that network traffic takes from its source to its destination. The route a datagram may follow can include many gateways and many physical networks.
In the Internet, each datagram is routed separately.

Router
A system is responsible for making decisions about which of several paths network (or Internet) traffic will follow. To do this, it uses a routing protocol to gain information about the network and algorithms to choose the best route based on several criteria known as "routing metrics".

Routing Table
Information stored within a router that contains network path and status information. It is used to select the most appropriate route to forward information along.

Routing Information Protocol
Routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.

SNMP
Simple Network Management Protocol - The network management protocol of choice for TCP/IP-based Internet.

SOCKET
(1) The Berkeley UNIX mechanism for creating a virtual connection between processes.
(2) IBM term for software interfaces that allow two UNIX application programs to talk via TCP/IP protocols.

Spanning-Tree Bridge Protocol (STP)
Spanning-Tree Bridge Protocol (STP) - Part of an IEEE standard. A mechanism for detecting and preventing loops from occurring in a multi-bridged environment.
When three or more LAN's segments are connected via bridges, a loop can occur. Because of a bridge forwards all packets that are not recognized as being local,
some packets can circulate for long periods of time, eventually degrading system performance. This algorithm ensures only one path connects any pair of stations, selecting one bridge as the 'root' bridge, with the highest priority one as identifier, from which all paths should radiate.

Spoofing
A method of fooling network end stations into believing that keep alive signals have come from and returned to the host. Polls are received and returned locally at
either end

Static IP Address
A static IP address is an IP address permanently assigned to computer in a TCP/IP network. Static IP addresses are usually assigned to networked devices that are consistently accessed by multiple users, such as Server PCs, or printers. If you are using your Router to share your cable or DSL Internet connection, contact your ISP to see if they have assigned your home a static IP address. You will need that address during your Router's configuration.

Subnet
For routing purposes, IP networks can be divided into logical subnets by using a subnet mask. Values below those of the mask are valid addresses on the subnet.

TCP
Transmission Control Protocol - The major transport protocol in the Internet suite of protocols provides reliable, connection-oriented full-duplex streams.

TFTP
Trivial File Transfer Protocol. A simple file transfer protocol (a simplified version of FTP) that is often boot diskless workstations and other network devices such as routers over a network (typically a LAN).

Telnet
The virtual terminal protocol in the Internet suite of protocols - Allows users of one host to log into a remote host and act as normal terminal users of that host.

Transparent bridging
The intelligence necessary to make relaying decisions exists in the bridge itself and is thus transparent to the communicating workstations. It involves frame forwarding, learning workstation addresses, and ensuring no topology loops exist (in conjunction with the Spanning-Tree algorithm).

UDP
User Datagram Protocol - A connectionless transport protocol that runs on top of TCP/IP's IP. UDP, like TCP, uses IP for delivery; however, unlike TCP, UDP provides for exchange of datagram without acknowledgments or guaranteed delivery. Best suited for small, independent requests, such as requesting a MIB value from an SNMP agent, in which first

setting up a connection would take more time than sending the data.

UNI signaling
User Network Interface signaling for ATM communications.

Virtual Connection (VC)
A link that seems and behaves like a dedicated point-to-point line or a system that delivers packets in sequence, as happens on an actual point-to-point network. In reality, the data is delivered across a network via the most appropriate route. The sending and receiving devices do not have to be aware of the options and the route is chosen only when a message is sent. There is no pre-arrangement, so each virtual connection exists only for the duration of that one transmission.

WAN
Wide area network - A data communications network that spans any distance and is usually provided by a public carrier (such as a telephone company or service provider)